



Release Notes for the Catalyst 3750, 3560, and 2960 Switches, Cisco IOS Release 12.2(46)SE

Revised January 21, 2009

Cisco IOS Release 12.2(46)SE and later runs on all Catalyst 3750, 3560, and 2960 switches and on Cisco EtherSwitch service modules.

The Catalyst 3750 switches and the Cisco EtherSwitch service modules support stacking through Cisco StackWise technology. The Catalyst 3560 and 2960 switches do not support switch stacking. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

These release notes include important information about Cisco IOS Release 12.2(46)SE and later and any limitations, restrictions, and caveats that apply to the releases. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the “[Finding the Software Version and Feature Set](#)” section on page 7.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the “[Deciding Which Files to Use](#)” section on page 7.

For the complete list of Catalyst 3750, 3560, and 2960 switch documentation and of Cisco EtherSwitch service module documentation, see the “[Related Documentation](#)” section on page 59.

You can download the switch software from this site (registered Cisco.com users with a login password):
<http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml>

This software release is part of a special release of Cisco IOS software that is not released on the same maintenance cycle that is used for other platforms. As maintenance releases and future software releases become available, they will be posted to Cisco.com in the Cisco IOS software area.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008–2009 Cisco Systems, Inc. All rights reserved.

Contents

This information is in the release notes:

- [System Requirements, page 2](#)
- [Upgrading the Switch Software, page 7](#)
- [Installation Notes, page 12](#)
- [New Features, page 13](#)
- [Minimum Cisco IOS Release for Major Features, page 14](#)
- [Limitations and Restrictions, page 19](#)
- [Important Notes, page 35](#)
- [Open Caveats, page 38](#)
- [Resolved Caveats, page 40](#)
- [Documentation Updates, page 43](#)
- [Obtaining Documentation and Submitting a Service Request, page 61](#)

System Requirements

The system requirements are described in these sections:

- [Hardware Supported, page 2](#)
- [Device Manager System Requirements, page 5](#)
- [Cluster Compatibility, page 6](#)
- [CNA Compatibility, page 6](#)

Hardware Supported

[Table 1](#) lists the hardware supported on this release.

Table 1 *Catalyst 3750, 3560 and 2960 Switches and Cisco EtherSwitch Service Modules Supported Hardware*

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 3750G-24WS-S25	24 10/100/1000 PoE ¹ ports, 2 SFP ² module slots, and an integrated wireless LAN controller supporting up to 25 access points.	Cisco IOS Release 12.2(25)FZ or Cisco IOS Release 12.2(35)SE
Catalyst 3750G-24WS-S50	24 10/100/1000 PoE ports, 2 SFP module slots, and an integrated wireless LAN controller supporting up to 50 access points	Cisco IOS Release 12.2(25)FZ or Cisco IOS Release 12.2(35)SE
Catalyst 3750-24FS	24 100BASE-FX ports and 2 SFP module slots	Cisco IOS Release 12.2(25)SEB
Catalyst 3750-24PS	24 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750-24TS	24 10/100 Ethernet ports and 2 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750-48PS	48 10/100 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE

Table 1 *Catalyst 3750, 3560 and 2960 Switches and Cisco EtherSwitch Service Modules Supported Hardware*

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 3750-48TS	48 10/100 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-12S	12 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-16TD	16 10/100/1000 Ethernet ports and 1 XENPAK 10-Gigabit Ethernet module slot	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-24PS	24 10/100/1000 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3750G-24T	24 10/100/1000 Ethernet ports	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-24TS	24 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3750G-24TS-1U	24 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3750G-48PS	48 10/100/1000 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3750G-48TS	48 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560-8PC	8 10/100 PoE ports and 1 dual-purpose port ³ (one 10/100/1000BASE-T copper port and one SFP module slot)	Cisco IOS Release 12.2(35)SE
Catalyst 3560-24PS	24 10/100 PoE ports and 2 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3560-24TS	24 10/100 ports and 2 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560-48PS	48 10/100 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(18)SE
Catalyst 3560-48TS	48 10/100 ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-24PS	24 10/100 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-24TS	24 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-48PS	48 10/100/1000 PoE ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-48TS	48 10/100/1000 Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(20)SE3
Catalyst 2960-8TC-S	8 10/100 ports and 1 dual-purpose port ³ (1 10/100/1000BASE-T copper port and 1 SFP module slot)	Cisco IOS Release 12.2(46)SE
Catalyst 2960-48TT-S	48 10/100 ports and 2 10/100/1000 ports	Cisco IOS Release 12.2(46)SE
Catalyst 2960-48PST-L	48 10/100 PoE ports, 2 10/100/1000 ports and 2 SFP module slots	Cisco IOS Release 12.2(46)SE
Catalyst 2960PD-8TT-L	8 10/100 ports and 1 10/100/1000 port that receives power	Cisco IOS Release 12.2(44)SE
Catalyst 2960-24LT-L	24 10/100 ports, 8 of which are PoE, and 2 10/100/1000 ports	Cisco IOS Release 12.2(44)SE
Catalyst 2960-24PC-L	24 10/100 Power over Ethernet (PoE) ports and 2 dual-purpose ports (2 10/100/1000BASE-T copper ports and 2 small form-factor pluggable [SFP] module slots)	Cisco IOS Release 12.2(44)SE

Table 1 Catalyst 3750, 3560 and 2960 Switches and Cisco EtherSwitch Service Modules Supported Hardware

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 2960-24-S	24 10/100 BASE-TX Ethernet ports	Cisco IOS Release 12.2(37)EY
Catalyst 2960-24TC-S	24 10/100BASE-T Ethernet ports and 2 dual-purpose ports (two 10/100/1000BASE-T copper ports and two SFP module slots)	Cisco IOS Release 12.2(37)EY
Catalyst 2960-48TC-S	48 10/100BASE-T Ethernet ports and 2 dual-purpose ports (two 10/100/1000BASE-T copper ports and two SFP module slots)	Cisco IOS Release 12.2(37)EY
Catalyst 2960-8TC-L	8 10/100 Ethernet ports and 1 dual-purpose port (one 10/100/1000BASE-T copper port and one SFP module slot)	Cisco IOS Release 12.2(35)SE
Catalyst 2960G-8TC-L	7 10/100/1000 Ethernet ports and 1 dual-purpose port (one 10/100/1000BASE-T copper port and one SFP module slot)	Cisco IOS Release 12.2(35)SE
Catalyst 2960-48TC-L	48 10/100BASE-TX Ethernet ports and 2 dual-purpose ports	Cisco IOS Release 12.2(25)FX
Catalyst 2960-24TC-L	24 10/100BASE-TX Ethernet ports and 2 dual-purpose ports	Cisco IOS Release 12.2(25)FX
Catalyst 2960-24TT-L	24 10/100BASE-T Ethernet ports and 2 10/100/1000BASE-T Ethernet ports	Cisco IOS Release 12.2(25)FX
Catalyst 2960-48TT-L	48 10/100BASE-T Ethernet ports 2 10/100/1000BASE-T Ethernet ports	Cisco IOS Release 12.2(25)FX
Catalyst 2960G-24TC-L	24 10/100/1000BASE-T Ethernet ports, including 4 dual-purpose ports (four 10/100/1000BASE-T copper ports and four SFP module slots)	Cisco IOS Release 12.2(25)FX
Catalyst 2960G-48TC-L	48 10/100/1000BASE-T Ethernet ports, including 4 dual-purpose ports (four 10/100/1000BASE-T copper ports and four SFP module slots)	Cisco IOS Release 12.2(25)SEE
NME-16ES-1G ⁴	16 10/100 ports, 1 10/100/1000 Ethernet port, no StackWise connector ports, single-wide	Cisco IOS Release 12.2(25)SEC
NME-16ES-1G-P ⁴	16 10/100 PoE ports, 1 10/100/1000 Ethernet port, no StackWise connector ports, single-wide	Cisco IOS Release 12.2(25)EZ
NME-X-23ES-1G ⁴	23 10/100 ports, 1 10/100/1000 PoE port, no StackWise connector ports, extended single-wide	Cisco IOS Release 12.2(25)SEC
NME-X-23ES-1G-P ⁴	23 10/100 PoE ports, 1 10/100/1000 PoE port, no StackWise connector ports, extended single-wide	Cisco IOS Release 12.2(25)EZ
NME-XD-24ES-1S-P ⁴	24 10/100 PoE ports, 1 SFP module port, 2 StackWise connector ports, extended double-wide	Cisco IOS Release 12.2(25)EZ
NME-XD-48ES-2S-P ⁴	48 10/100 PoE ports, 2 SFP module ports, no StackWise connector ports, extended double-wide	Cisco IOS Release 12.2(25)EZ
SFP modules (Catalyst 3750 and 3560)	1000BASE-CWDM ⁵ , -LX, SX, -T, -ZX 100BASE-FX MMF ⁶	Cisco IOS Release 12.2(18)SE Cisco IOS Release 12.2(20)SE

Table 1 Catalyst 3750, 3560 and 2960 Switches and Cisco EtherSwitch Service Modules Supported Hardware

Switch	Description	Supported by Minimum Cisco IOS Release
SFP modules (Catalyst 2960)	1000BASE-BX, -CWDM, -LX/LH, -SX, -ZX 100BASE-BX, FX, -LX	Cisco IOS Release 12.2(25)FX
XENPAK modules ⁷	XENPAK-10-GB-ER, XENPAK-10-GB-LR, and XENPAK-10-GB-SR	Cisco IOS Release 12.2(18)SE
Redundant power systems	Cisco RPS 675 Redundant Power System Cisco RPS 300 Redundant Power System (supported only on the Catalyst 2960 switch) Cisco Redundant Power System 2300	Supported on all software releases Supported on all software releases Cisco IOS Release 12.2(35)SE and later

- PoE = Power over Ethernet
- SFP = small form-factor pluggable
- Each uplink port is considered a single interface with dual front ends (RJ-45 connector and SFP module slot). The dual front ends are not redundant interfaces, and only one port of the pair is active.
- Cisco EtherSwitch service module
- CWDM = coarse wavelength-division multiplexer
- MMF = multimode fiber
- XENPAK modules are only supported on the Catalyst 3750G-16TD switches.

Device Manager System Requirements

These sections describes the hardware and software requirements for using the device manager:

- [Hardware Requirements, page 5](#)
- [Software Requirements, page 6](#)

Hardware Requirements

[Table 2](#) lists the minimum hardware requirements for running the device manager.

Table 2 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum ¹	512 MB ²	256	1024 x 768	Small

- We recommend 1 GHz.
- We recommend 1 GB DRAM.

Software Requirements

Table 3 lists the supported operating systems and browsers for using the device manager. The device manager verifies the browser version when starting a session to ensure that the browser is supported.


Note

The device manager does not require a plug-in.

Table 3 **Supported Operating Systems and Browsers**

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer ¹	Netscape Navigator
Windows 2000	None	5.5 or 6.0	7.1
Windows XP	None	5.5 or 6.0	7.1

1. Service Pack 1 or higher is required for Internet Explorer 5.5.

Cluster Compatibility

You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the command-line interface (CLI) or the Network Assistant application.

When creating a switch cluster or adding a switch to a cluster, follow these guidelines:

- When you create a switch cluster, we recommend configuring the highest-end switch in your cluster as the command switch.
- If you are managing the cluster through Network Assistant, the switch with the latest software should be the command switch.
- The standby command switch must be the same type as the command switch. For example, if the command switch is a Catalyst 3750 switch, all standby command switches must be Catalyst 3750 switches.

For additional information about clustering, see *Getting Started with Cisco Network Assistant* and *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com), the software configuration guide, the command reference, and the Cisco EtherSwitch service module feature guide.

CNA Compatibility

Cisco IOS 12.2(46)SE is only compatible with Cisco Network Assistant (CNA) 5.0 and later. You can download Cisco Network Assistant from this URL:

<http://www.cisco.com/pcgi-bin/tablebuild.pl/NetworkAssistant>

For more information about Cisco Network Assistant, see the *Release Notes for Cisco Network Assistant* on Cisco.com.

Upgrading the Switch Software

These are the procedures for downloading software. Before downloading software, read this section for important information:

- [Finding the Software Version and Feature Set, page 7](#)
- [Deciding Which Files to Use, page 7](#)
- [Catalyst 3750G Integrated Wireless LAN Controller Switch Software Compatibility, page 9](#)
- [Archiving Software Images, page 10](#)
- [Upgrading a Switch by Using the Device Manager or Network Assistant, page 10](#)
- [Upgrading a Switch by Using the CLI, page 11](#)
- [“Recovering from a Software Failure” section on page 12](#)

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. The image is stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.



Note

For Catalyst 3750 and 3560 switches and the Cisco EtherSwitch service modules, although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration (IP base image [formerly known as the SMI] or IP services image [formerly known as the EMI]) and does not change if you upgrade the software image.

You can also use the **dir filesystem:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains the Cisco IOS image file and the files needed for the embedded device manager. You must use the combined tar file to upgrade the switch through the device manager. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

For the Catalyst 3750 and 3560 switches, Cisco IOS Release 12.2(25)SEA and earlier referred to the image that provides Layer 2+ features and basic Layer 3 routing as the standard multilayer image (SMI). The image that provides full Layer 3 routing and advanced services was referred to as the enhanced multilayer image (EMI).

Cisco IOS Release 12.2(25)SEB and later refers to the SMI as the *IP base* image and the EMI as the *IP services* image.

Table 4 lists the different file-naming conventions before and after Cisco IOS Release 12.2(25)SEB.

Table 4 Cisco IOS Image File Naming Convention

Cisco IOS 12.2(25)SEA and earlier	Cisco IOS 12.2(25)SEB and later
c3750-i9-mz (SMI ¹)	c3750-ipbase-mz
c3750-i9k91-mz (SMI)	c3750-ipbasek9-mz
c3750-i5-mz (EMI ²)	c3750-ipservices-mz
c3750-i5k91-mz (EMI)	c3750-ipservicesk9-mz
c3560-i9-mz (SMI)	c3560-ipbase-mz
c3560-i9k91-mz (SMI)	c3560-ipbasek9-mz
c3560-i5-mz (EMI)	c3560-ipservices-mz
c3560-i5k91-mz (EMI)	c3560-ipservicesk9-mz

1. SMI = standard multilayer image
2. EMI = enhanced multilayer image

Table 5 lists the filenames for this software release.



Note

For IPv6 capability on the Catalyst 3750 or 3560 switch or on the Cisco EtherSwitch service modules, you must order the advanced IP services image upgrade from Cisco.

Table 5 Cisco IOS Software Image Files

Filename	Description
c3750-ipbase-tar.122-46.SE2.tar	Catalyst 3750 IP base image and device manager files. This image has Layer 2+ and basic Layer 3 routing features. This image also runs on the Cisco EtherSwitch service modules.
c3750-ipservices-tar.122-46.SE.tar	Catalyst 3750 IP services image and device manager files. This image has both Layer 2+ and full Layer 3 routing features. This image also runs on the Cisco EtherSwitch service modules.
c3750-ipbasek9-tar.122-46.SE.tar	Catalyst 3750 IP base cryptographic image and device manager files. This image has the Kerberos, SSH ¹ , Layer 2+, and basic Layer 3 routing features. This image also runs on the Cisco EtherSwitch service modules.
c3750-ipservicesk9-tar.122-46.SE.tar	Catalyst 3750 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features. This image also runs on the Cisco EtherSwitch service modules.
c3750-advipservicesk9-tar.122-46.SE.tar	Catalyst 3750 advanced IP services image, cryptographic file, and device manager files. This image has all the IP services image (formerly known as the EMI) features and the capability for unicast routing of IPv6 packets. This image also runs on the Cisco EtherSwitch service modules.
c3560-ipbase-tar.122-46.SE.tar	Catalyst 3560 IP base image file and device manager files. This image has Layer 2+ and basic Layer 3 routing features.

Table 5 Cisco IOS Software Image Files (continued)

Filename	Description
c3560-ipservices-tar.122-46.SE.tar	Catalyst 3560 IP services image and device manager files. This image has both Layer 2+ and full Layer 3 routing features.
c3560-ipbasek9-tar.122-46.SE.tar	Catalyst 3560 IP base cryptographic image and device manager files. This image has the Kerberos, SSH, and Layer 2+, and basic Layer 3 routing features.
c3560-ipservicesk9-tar.122-46.SE.tar	Catalyst 3560 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features.
c3560-advipservicesk9-tar.122-46.SE.tar	Catalyst 3560 advanced IP services image, cryptographic file, and device manager files. This image has all the IP services image (formerly known as the EMI) features and the capability for unicast routing of IPv6 packets.
c2960-lanbase-tar.122-46.SE.tar	Catalyst 2960 image file and device manager files. This image has Layer 2+ features.
c2960-lanbasek9-tar.122-46.SE.tar	Catalyst 2960 cryptographic image file and device manager files. This image has the Kerberos and SSH features.
c2960-lanlitek9-tar.122-46.SE.tar	Catalyst 2960 LAN lite cryptographic image file and device manager files.
c2960-lanlite-tar.122-46.SE.tar	Catalyst 2960 LAN lite image file and device manager files.

1. SSH = Secure Shell

Catalyst 3750G Integrated Wireless LAN Controller Switch Software Compatibility

The Catalyst 3750 Integrated Wireless LAN Controller Switch is an integrated Catalyst 3750 switch and Cisco 4400 series wireless LAN controller that supports up to 25 or 50 lightweight access points. The switch and the internal controller run separate software versions, which must be upgraded separately.

To use the controller in the Catalyst 3750G Wireless LAN Controller Switch, the switch must be running one of these Cisco IOS software releases:

- Cisco IOS Release 12.2(25)FZ
- Cisco IOS Release 12.2(35)SE or later
- Cisco IOS Release 12.2(37)SE or later
- Cisco IOS Release 12.2(44)SE or later
- Cisco IOS Release 12.2(46)SE or later



Note

These Cisco IOS Releases and any versions of them are not supported: Cisco IOS Release 12.2(25)SEC, 12.2(25)SED, 12.2(25)SEE, 12.2(25)SEF, and 12.2(25)SEG. All Catalyst 3750 images (IP Base, IP Services, and Advanced IP Services) are supported for use with the controller.

If the switch image version is not compatible, the wireless LAN controller switch could stop functioning.

For information about the controller software, see the release notes on this page for Cisco Software Release 4.0.x.0 or later:

http://www.cisco.com/en/US/products/ps6366/prod_release_notes_list.html

For controller software upgrade procedure, see the *Cisco Wireless LAN Controller Configuration Guide* on this page:

http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html

Archiving Software Images

Before upgrading your switch software, make sure that you have archived copies of the current Cisco IOS release and the Cisco IOS release to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_bulletin0900aecd80281c0e.html

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.



Note

Although you can copy any file on the flash memory to the TFTP server, it is time consuming to copy all of the HTML files in the tar file. We recommend that you download the tar file from Cisco.com and archive it on an internal host in your network.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the “Basic File Transfer Services Commands” section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca744.html

Upgrading a Switch by Using the Device Manager or Network Assistant

You can upgrade switch software by using the device manager or Network Assistant. For detailed instructions, click **Help**.



Note

When using the device manager to upgrade your switch, do not use or close your browser session after the upgrade process begins. Wait until after the upgrade process completes.

Upgrading a Switch by Using the CLI

This procedure is for copying the combined tar file to the switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

To download software, follow these steps:

-
- Step 1** Use [Table 5 on page 8](#) to identify the file that you want to download.
- Step 2** Download the software image file. If you have a SmartNet support contract, go to this URL, and log in to download the appropriate files:

<http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml>

To download the image for a Catalyst 2960 switch, click **Catalyst 2960 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 2960 3DES Cryptographic Software**.

To download the IP services image (formerly known as the EMI) or IP base image (formerly known as the SMI) files for a Catalyst 3560 switch, click **Catalyst 3560 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 3560 3DES Cryptographic Software**.

To download the IP services image (formerly known as the EMI) or IP base image (formerly known as the SMI) files for a Catalyst 3750 switch, click **Catalyst 3750 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 3750 3DES Cryptographic Software**.



Caution

If you are upgrading a Catalyst 3750 switch that is running a release earlier than Cisco IOS Release 12.1(19)EA1c, this release includes a bootloader upgrade. The bootloader can take up to 1 minute to upgrade the first time that the new software is loaded. Do not power cycle the switch during the bootloader upgrade.

- Step 3** Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.
- For more information, see Appendix B in the software configuration guide for this release.
- Step 4** Log into the switch through the console port or a Telnet session.
- Step 5** (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
Switch# ping tftp-server-address
```

For more information about assigning an IP address and default gateway to the switch, see the software configuration guide for this release.

- Step 6** Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by entering this privileged EXEC command:

```
Switch# archive download-sw /overwrite /reload
tftp: [[/location]/directory]/image-name.tar
```

The **/overwrite** option overwrites the software image in flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.

For *///location*, specify the IP address of the TFTP server.

For */directory/image-name.tar*, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite
tftp://198.30.20.19/c3750-ipservices-tar.122-46.SE.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

Recovering from a Software Failure

For additional recovery procedures, see the “Troubleshooting” chapter in the software configuration guide for this release.

Installation Notes

You can assign IP information to your switch by using these methods:

- The Express Setup program, as described in the switch getting started guide.
- The CLI-based setup program, as described in the switch hardware installation guide.
- The DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manually assigning an IP address, as described in the switch software configuration guide.



Note

If you are upgrading a Catalyst 3750 or a 2950 switch running Cisco IOS Release 12.1(11)AX, which uses the IEEE 802.1x feature, you must re-enable IEEE 802.1x after upgrading the software. For more information, see the [“Cisco IOS Notes” section on page 35](#).



Note

When upgrading or downgrading from Cisco IOS Release 12.2(18)SE, you might need to reconfigure the switch with the same password that you were using when running Cisco IOS Release 12.2(18)SE. This problem only occurs when changing from Cisco IOS Release 12.2(18)SE to any other release. (CSCed88768)

New Features

This section describes the new and updated software features provided in this release:

New Software Features

These sections describe the new software features for this release:

- [Catalyst 3750, 3560, and 2960 switches, page 13](#)
- [Catalyst 3750 and 3560 Switches, page 13](#)
- [Catalyst 2960 switch, page 14](#)

Catalyst 3750, 3560, and 2960 switches

These are the new features for the Catalyst 3750, 3560, and 2960 switches:

- Generic message authentication support with the SSH Protocol and compliance with RFC 4256
- Disabling MAC address learning on a VLAN
- PAgP Interaction with Virtual Switches and Dual-Active Detection, also referred to as enhanced PAgP
- DHCP server port-based address allocation for the preassignment of an IP address to a switch port
- IPv6 default router preference (DRP) for improving the ability of a host to select an appropriate router

Catalyst 3750 and 3560 Switches

These are the new features for the Catalyst 3750 and 3560 switches:

- Voice aware IEEE 802.1x and mac authentication bypass (MAB) security violation to shut down only the data VLAN on a port when a security violation occurs
- Local web authentication banner so that custom banner or image file can be displayed at a web authentication login screen
- Support for the CISCO-NAC-NAD and CISCO-PAE MIBs
- The ability to exclude a port in a VLAN from the SVI line-state up or down calculation
- EOT and IP SLAs EOT static route support to identify when a preconfigured static route or a DHCP route goes down
- Support for HSRP Version 2 (HSRPv2)
- HSRP for IPv6 (requires the advanced IP services image)
- DHCP for IPv6 relay, client, server address assignment and prefix delegation (requires the advanced IP services image)

Catalyst 2960 switch

These features were added to the Catalyst 2960 switch LAN Lite image:

- Dynamic voice virtual LAN (VLAN) for multidomain authentication (MDA) to allow a dynamic voice VLAN on an MDA-enabled port
- The ability to monitor and police the real-time power consumption on a per-PoE port basis
- IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute

Minimum Cisco IOS Release for Major Features

Table 6 lists the minimum software release required to support the major features of the Catalyst 3750, 3560, and 2960 switches and the Cisco EtherSwitch service modules.

Table 6 *Catalyst 3750, 3560, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required*

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Generic message authentication support with the SSH Protocol and compliance with RFC 4256	12.2(46)SE	3750, 3560, 2960
Generic message authentication support	12.2(46)SE	3750, 3560, 2960
Disabling MAC address learning on a VLAN	12.2(46)SE	3750, 3560, 2960
PAgP Interaction with Virtual Switches and Dual-Active Detection	12.2(46)SE	3750, 3560, 2960
DHCP server port-based address allocation	12.2(46)SE	3750, 3560, 2960
IPv6 default router preference (DRP)	12.2(46)SE	3750, 3560, 2960
Voice aware IEEE 802.1x and mac authentication bypass (MAB) security violation	12.2(46)SE	3750, 3560
Local web authentication banner	12.2(46)SE	3750, 3560
Support for the CISCO-NAC-NAD and CISCO-PAE MIBs	12.2(46)SE	3750, 3560
Exclude a port in a VLAN from the SVI line-state up or down calculation	12.2(46)SE	3750, 3560
EOT and IP SLAs EOT static route support	12.2(46)SE	3750, 3560
Support for HSRP Version 2 (HSRPv2)	12.2(46)SE	3750, 3560
HSRP for IPv6 (requires the advanced IP services image)	12.2(46)SE	3750, 3560
DHCP for IPv6 relay, client, server address assignment and prefix delegation (requires the advanced IP services image)	12.2(46)SE	3750, 3560
Embedded event manager (EEM) for device and system management (IP services image only)	12.2(46)SE	3750, 3560
Dynamic voice virtual LAN (VLAN) for multidomain authentication (MDA)	12.2(46)SE	2960
Monitor and police the real-time power consumption on a per-PoE port basis	12.2(46)SE	2960
IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute	12.2(46)SE	2960
IEEE 802.1x readiness check	12.2(44)SE	3750, 3560, 2960

Table 6 *Catalyst 3750, 3560, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)*

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
DHCP-based autoconfiguration and image update	12.2(44)SE	3750, 3560, 2960
Configurable small-frame arrival threshold	12.2(44)SE	3750, 3560, 2960
HTTP and HTTP(s) support over IPV6	12.2(44)SE	3750, 3560, 2960
Simple Network and Management Protocol (SNMP) configuration over IPv6 transport	12.2(44)SE	3750, 3560, 2960
IPv6 stateless autoconfiguration	12.2(44)SE	3750, 3560, 2960
Flex Link Multicast Fast Convergence	12.2(44)SE	3750, 3560, 2960
Digital optical monitoring (DOM)	12.2(44)SE	3750, 3560
Source Specific Multicast (SSM) mapping	12.2(44)SE	3750, 3560
/31 bit mask support for multicast traffic	12.2(44)SE	3750, 3560
Configuration replacement and rollback	12.2(40)SE	3750, 3560, 2960
Link Layer Discovery Protocol Media Extensions (LLDP-MED)	12.2(40)SE	3750, 3560, 2960
Support for Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6	12.2(40)SE	3750, 3560
Automatic quality of service (QoS) Voice over IP (VoIP)	12.2(40)SE	3750, 3560, 2960
Dynamic voice virtual LAN (VLAN) for multidomain authentication (MDA)-enabled ports	12.2(40)SE	3750, 3560
Internet Group Management Protocol (IGMP) helper	12.2(40)SE	3750, 3560
IP Service Level Agreements (IP SLAs)	12.2(40)SE	3750, 3560
IP SLAs EOT	12.2(40)SE	3750, 3560
Multicast virtual routing and forwarding (VRF) lite	12.2(40)SE	3750, 3560
SSM PIM protocol	12.2(40)SE	3750, 3560
VRF-aware support for these IP services: HSRP, uRPF, ARP, SNMP, IP SLA, TFTP, FTP, syslog, traceroute, and ping	12.2(40)SE	3750, 3560
MLD snooping	12.2(40)SE	2960
IPv6 host	12.2(40)SE	2960
IP phone detection enhancement	12.2(37)SE	3750, 3560, 2960
Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED)	12.2(37)SE	3750, 3560, 2960
PIM stub routing	12.2(37)SE	3750, 3560
Port security on a PVLAN host	12.2(37)SE	3750, 3560
VLAN aware port security option	12.2(37)SE	3750, 3560, 2960
Support for auto rendezvous point (auto-RP) for multicast	12.2(37)SE	3750, 3560
VLAN Flex Links load balancing	12.2(37)SE	3750, 3560, 2960
Web Cache Communication Protocol (WCCP)	12.2(37)SE	3750, 3560
Multidomain authentication (MDA)	12.2(35)SE	3750, 3560

Table 6 *Catalyst 3750, 3560, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)*

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Web authentication	12.2(35)SE	3750, 3560, 2960
MAC inactivity aging	12.2(35)SE	3750, 3560, 2960
Support for IPv6 with Express Setup	12.2(35)SE	3750, 3560
Generic online diagnostics to test the hardware functionality of the supervisor engine	12.2(35)SE	3560
Stack MAC persistent timer and archive download enhancements	12.2(35)SE	3750
HSRP enhanced object tracking	12.2(35)SE	3750, 3560
OSPF and EIGRP Nonstop forwarding capability (IP services image only)	12.2(35)SE	3750
IPv6 router ACLs for inbound Layer 3 management traffic in the IP base and IP services image	12.2(35)SE	3750, 3560
Generic online diagnostics to test the hardware functionality of the supervisor engine	12.2(25)SEE	3750
DHCP Option 82 configurable remote ID and circuit ID	12.2(25)SEE	3750, 3560, 2960
EIGRP stub routing in the IP base image	12.2(25)SEE	3750, 3560
/31 bit mask support for unicast traffic	12.2(25)SEE	3750, 3560
Access SDM templates	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
IPv6 ACLs	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
IPv6 Multicast Listener Discovery (MLD) snooping	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
QoS hierarchical policy maps on a port	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules
NAC Layer 2 IEEE 802.1x validation	12.2(25)SED	3750, 3560, 2960 Cisco EtherSwitch service modules
NAC Layer 2 IP validation	12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules

Table 6 *Catalyst 3750, 3560, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)*

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
IEEE 802.1x inaccessible authentication bypass.	12.2(25)SED 12.2(25)SEE	3750, 3560 Cisco EtherSwitch service module 2960
IEEE 802.1x with restricted VLAN	12.2(25)SED	3750, 3560, 2960 Cisco EtherSwitch service modules
Budgeting power for devices connected to PoE ports	12.2(25)SEC	3750, 3560 Cisco EtherSwitch service modules
Multiple spanning-tree (MST) based on the IEEE 802.1s standard	12.2(25)SEC 12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules 2960
Unique device identifier (UDI)	12.2(25)SEC 12.2(25)SED	3750, 3560 Cisco EtherSwitch service modules 2960
VRF Lite	12.2(25)SEC	3750, 3560 Cisco EtherSwitch service modules
IEEE 802.1x with wake-on-LAN	12.2(25)SEC 12.2(25)SED	3750, 3560 2960, Cisco EtherSwitch service modules
Nonstop forwarding (NSF) awareness	12.2(25)SEC	3750, 3560 Cisco EtherSwitch service modules
Configuration logging	12.2(25)SEC 12.2(25)SED	3750, 3560 2960, Cisco EtherSwitch service modules
Secure Copy Protocol	12.2(25)SEC 12.2(25)SED	3750, 3560 2960, Cisco EtherSwitch service modules
Cross-stack EtherChannel	12.2(25)SEC	3750 Cisco EtherSwitch service modules

Table 6 *Catalyst 3750, 3560, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)*

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Support for configuring private-VLAN ports on interfaces that are configured for dynamic ARP inspection (IP base image [formerly known as the SMI] only)	12.2(25)SEB	3750, 3560
Support for IP source guard on private VLANs (IP base image [formerly known as the SMI] only)	12.2(25)SEB	3750, 3560
Support for configuring an IEEE 802.1x restricted VLAN	12.2(25)SED	3750, 3560, 2960
IGMP leave timer	12.2(25)SEB 12.2(25)SED	3750, 3560, 2960
IGMP snooping querier	12.2(25)SEA 12.2(25)FX	3750, 3560, 2960
Advanced IP services	12.2(25)SEA	3750, 3560
Support for DSCP transparency	12.2(25)SE 12.2(25)FX	3750, 3560, 2960
Support for VLAN-based QoS ¹ and hierarchical policy maps on SVIs ²	12.2(25)SE	3750, 3560
Device manager	12.2(25)SE 12.2(25)FX	3750, 3560, 2960
IEEE 802.1Q tunneling and Layer 2 protocol tunneling	12.2(25)SE	3750, 3560
Layer 2 point-to-point tunneling and Layer 2 point-to-point tunneling bypass	12.2(25)SE	3750, 3560
Support for SSL version 3.0 for secure HTTP communication (cryptographic images only)	12.2(25)SE 12.2(25)FX	3750, 3560, 2960
Support for configuring private-VLAN ports on interfaces that are configured for dynamic ARP inspection (IP services image [formerly known as the EMI] only)	12.2(25)SE	3750, 3560
Support for IP source guard on private VLANs (IP services image [formerly known as the EMI] only)	12.2(25)SE	3750, 3560
Cisco intelligent power management to limit the power allowed on a port, or pre-allocate (reserve) power for a port.	12.2(25)SE	3750, 3560
IEEE 802.1x accounting and MIBs (IEEE 8021-PAE-MIB and CISCO-PAE-MIB)	12.2(20)SE 12.2(25)FX	3750, 3560, 2960
Dynamic ARP inspection	12.2(20)SE	3750, 3560
Flex Links	12.2(20)SE 12.2(25)FX	3750, 3560, 2960
Software upgrade (device manager or Network Assistant only)	12.2(20)SE 12.2(25)FX	3750, 3560, 2960
IP source guard	12.2(20)SE	3750, 3560

Table 6 *Catalyst 3750, 3560, and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)*

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Private VLAN (IP services image [formerly known as the EMI] only)	12.2(20)SE	3750, 3560
SFP module diagnostic management interface	12.2(20)SE 12.2(25)FX	3750, 3560, 2960
Switch stack offline configuration	12.2(20)SE	3750
Stack-ring activity statistics	12.2(20)SE	3750
Smartports macros	12.2(18)SE 12.2(25)FX	3750, 3560, 2960
Generic online diagnostics (GOLD)	12.2(25)SEE	3750
Flex Links Preemptive Switchover	12.2(25)SEE	3750, 3560, 2960

1. QoS = quality of service

2. SVIs = switched virtual interfaces

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

This section contains these limitations:

- [Cisco IOS Limitations, page 19](#)
- [Device Manager Limitations, page 34](#)

Cisco IOS Limitations

Unless otherwise noted, these limitations apply to the Catalyst 3750, 3560, and 2960 switches and the Cisco EtherSwitch service modules:

- [Configuration, page 20](#)
- [Ethernet, page 22](#)
- [Fallback Bridging, page 23](#)
- [HSRP, page 23](#)
- [IP, page 24](#)
- [IP Telephony, page 24](#)
- [MAC Addressing, page 24](#)
- [MAC Addressing, page 24](#)
- [Multicasting, page 25](#)
- [Power, page 26](#)

- [QoS, page 27](#)
- [Routing, page 27](#)
- [SPAN and RSPAN, page 29](#)
- [Stacking \(Catalyst 3750 or Cisco EtherSwitch service module switch stack only\), page 31](#)
- [Trunking, page 33](#)
- [VLAN, page 34](#)

Configuration

These are the configuration limitations:

- A static IP address might be removed when the previously acquired DHCP IP address lease expires.

This problem occurs under these conditions:

- When the switch is booted up without a configuration (no config.text file in flash memory).
- When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).
- When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

The workaround is to reconfigure the static IP address. (CSCea71176 and CSCdz11708)

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) When the **show interface** privileged EXEC is entered on a port that is running IEEE 802.1Q, inconsistent statistics from ports running IEEE 802.1Q might be reported. The workaround is to upgrade to Cisco IOS Release 12.1(20)EA1. (CSCec35100)
- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) When you change a port from a nonrouted port to a routed port or the reverse, the applied auto-QoS setting is not changed or updated when you verify it by using the **show running interface** or **show mls qos interface** user EXEC commands. These are the workarounds:
 1. Disable auto-QoS on the interface.
 2. Change the routed port to a nonrouted port or the reverse.
 3. Re-enable auto-QoS on the interface. (CSCec44169)
- The DHCP snooping binding database is not written to flash memory or a remote file in any of these situations:
 - (Catalyst 3750 switch and Cisco EtherSwitch service modules) When the Network Time Protocol (NTP) is configured, but the NTP clock is not synchronized. You can check the clock status by entering the **show NTP status** privileged EXEC command and verifying that the network connection to the NTP server and the peer work correctly.
 - (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The DHCP snooping database file is manually removed from the file system. After enabling the DHCP snooping database by configuring a database URL, a database file is created. If the file is manually removed from the file system, the DHCP snooping database does not create another database file. You need to disable the DHCP snooping database and enable it again to create the database file.
 - (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The URL for the configured DHCP snooping database was replaced because the original URL was not accessible. The new URL might not take effect after the timeout of the old URL.

No workaround is necessary; these are the designed behaviors. (CSCed50819)

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) When dynamic ARP inspection is enabled on a switch or switch stack, ARP and RARP packets greater than 2016 bytes are dropped by the switch or switch stack. This is a hardware limitation.

However, when dynamic ARP inspection is not enabled and a jumbo MTU is configured, ARP and RARP packets are correctly bridged in hardware. (CSCed79734)

- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mb/s full duplex or 100 Mb/s half duplex might bounce the line protocol up and down. The problem is observed only when the switch is receiving frames.

The workaround is to configure the port for 10 Mb/s and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)

- (Catalyst 3750 switches and Cisco EtherSwitch service modules) Dynamic ARP inspection log entries might be lost after a switch failure. Any log entries that are still in the log buffer (have not been output as a system message) on a switch that fails are lost.

When you enter the **show ip arp inspection log** privileged EXEC command, the log entries from all switches in the stack are moved to the switch on which you entered the command.

There is no workaround. (CSCed95822)

- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked

The workaround is to enter the **no switchport block unicast** interface configuration command on that specific interface. (CSCee93822)

- A traceback error occurs if a crypto key is generated after an SSL client session.

There is no workaround. This is a cosmetic error and does not affect the functionality of the switch. (CSCef59331)

- (Cisco EtherSwitch service modules) You cannot change the console baud rate by using the switch CLI. The console on the Cisco EtherSwitch service modules only supports three baud rates (9600 b/s, 19200 b/s, and 38400 b/s) and must be set at the bootloader prompt. The switch rejects a CLI command to change the baud rate.

To change the baud rate, reload the Cisco EtherSwitch service module with the bootloader prompt. You can then change the baud rate and change the speed on the TTY line of the router connected to the Cisco EtherSwitch Service module console.

There is no workaround. (CSCeh50152)

- When a Catalyst 3750-12S switch boots up, ports 1, 2, 5, 6, 9, and 10 can become active before the Cisco IOS software loading process is complete. Packets arriving at these ports before the switch software is completely loaded are lost. This is a hardware limitation when the switch uses small form-factor pluggable (SFP) modules with copper connections.

The workaround is to use switch ports other than those specified for redundancy and for applications that immediately detect active links. (CSCeh70503)

- When the **logging event-spanning-tree** interface configuration command is configured and logging to the console is enabled, a topology change might generate a large number of logging messages, causing high CPU utilization. CPU utilization can increase with the number of spanning-tree instances and the number of interfaces configured with the **logging event-spanning-tree** interface configuration command. This condition adversely affects how the switch operates and could cause problems such as STP convergence delay.

High CPU utilization can also occur with other conditions, such as when debug messages are logged at a high rate to the console.

Use one of these workarounds:

- Disable logging to the console.
- Rate-limit logging messages to the console.
- Remove the **logging event spanning-tree** interface configuration command from the interfaces. (CSCsg91027)
- The switch might display tracebacks similar to this example when an EtherChannel interface port-channel type changes from Layer 2 to Layer 3 or the reverse:


```
15:50:11: %COMMON_FIB-4-FIBNULLHWIDB: Missing hwidb for fibhwidb Port-channel1
(ifindex 1632) -Traceback= A585C B881B8 B891CC 2F4F70 5550E8 564EAC 851338 84AF0C
4CEB50 859DF4 A7BF28 A98260 882658 879A58
(CSCsh12472 [Catalyst 3750 and 3560 switches])
```
- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module. The workaround is to configure aggressive UDLD. (CSCsh70244).
- A ciscoFlashMIBTrap message appears during switch startup. This does not affect switch functionality. (CSCsj46992)
- When authorization and accounting are enabled on the switch and you use the **interface range** command to change the configuration on a range of interfaces, the change might cause high CPU utilization and authentication failures.

The workaround is to disable authorization and accounting or to enter the configuration change for one interface at a time. (CSCsg80238, CSCti76748)

Ethernet

These are the Ethernet limitations:

- Link connectivity might be lost between some older models of the Intel Pro1000 NIC and the 10/100/1000 switch port interfaces. The loss of connectivity occurs between the NIC and these switch ports:
 - Ports 3, 4, 7, 8, 11, 12, 15, 16, 19, 20, 23, and 24 of the Catalyst 3750G-24T and 3750G-24TS switches
 - Gigabit Ethernet ports on the Cisco EtherSwitch service modules

These are the workarounds:

- Contact the NIC vendor, and get the latest driver for the card.
- Configure the interface for 1000 Mb/s instead of for 10/100 Mb/s.
- Connect the NIC to an interface that is not listed here. (CSCea77032)

For more information, enter *CSCea77032* in the Bug Toolkit at this URL:

<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>

- (Cisco EtherSwitch service modules) When a Cisco EtherSwitch service module reloads or the internal link resets, there can be up to a 45-second delay in providing power to PoE devices, depending on the configuration. If the internal Gigabit Ethernet interface on a Cisco EtherSwitch service module connected to the router is configured as a switch port in access mode or in trunk mode, the internal link is not operational until it reaches the STP forwarding state. Therefore, the

PoE that comes from the host router is also not available until the internal Gigabit Ethernet link reaches the STP forwarding state. This is due to STP convergence time. This problem does not occur on routed ports.

If the Cisco EtherSwitch service module is in access mode, the workaround is to enter the **spanning-tree portfast** interface configuration command on the internal Gigabit Ethernet interface. If the service module is in trunk mode, there is no workaround.

- Traffic on EtherChannel ports is not perfectly load-balanced. Egress traffic on EtherChannel ports are distributed to member ports on load balance configuration and traffic characteristics like MAC or IP address. More than one traffic stream may map to same member ports based on hashing results calculated by the ASIC.

If this happens, uneven traffic distribution will happen on EtherChannel ports.

Changing the load balance distribution method or changing the number of ports in the EtherChannel can resolve this problem. Use any of these workarounds to improve EtherChannel load balancing:

- for random source-ip and dest-ip traffic, configure load balance method as **src-dst-ip**
- for incrementing source-ip traffic, configure load balance method as **src-ip**
- for incrementing dest-ip traffic, configure load balance method as **dst-ip**
- Configure the number of ports in the EtherChannel so that the number is equal to a power of 2 (i.e. 2, 4, or 8)

For example, with load balance configured as **dst-ip** with 150 distinct incrementing destination IP addresses, and the number of ports in the EtherChannel set to either 2, 4, or 8, load distribution is optimal.(CSCeh81991)

Fallback Bridging

These are the fallback bridging limitations:

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) If a bridge group contains a VLAN to which a static MAC address is configured, all non-IP traffic in the bridge group with this MAC address destination is sent to all ports in the bridge group. The workaround is to remove the VLAN from the bridge group or to remove the static MAC address from the VLAN. (CSCdw81955)
- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) Known unicast (secured) addresses are flooded within a bridge group if secure addresses are learned or configured on a port and the VLAN on this port is part of a bridge group. Non-IP traffic destined to the secure addresses is flooded within the bridge group. The workaround is to disable fallback bridging or to disable port security on all ports in all VLANs participating in fallback bridging. To remove an interface from a bridge group and to remove the bridge group, use the **no bridge-group bridge-group** interface configuration command. To disable port security on all ports in all VLANs participating in fallback bridging, use the **no switchport port-security** interface configuration command. (CSCdz80499)

HSRP

This is the Hot Standby Routing Protocol (HSRP) limitation:

When the active switch fails in a switch cluster that uses HSRP redundancy, the new active switch might not contain a full cluster member list. The workaround is to ensure that the ports on the standby cluster members are not in the spanning-tree blocking state. To verify that these ports are not in the blocking state, see the “Configuring STP” chapter in the software configuration guide. (CSCec76893)

IP

These are the IP limitations:

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The switch does not create an adjacent table entry when the ARP timeout value is 15 seconds and the ARP request times out. The workaround is to not set an ARP timeout value lower than 120 seconds. (CSCea21674)
- When the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console. The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring. (CSCeb59166)

IP Telephony

These are the IP telephony limitations:

- After you change the access VLAN on a port that has IEEE 802.1x enabled, the IP phone address is removed. Because learning is restricted on IEEE 802.1x-capable ports, it takes approximately 30 seconds before the address is relearned. No workaround is necessary. (CSCea85312)
- (Catalyst 3750 or 3560 PoE-capable switches and Cisco EtherSwitch service modules) The switch uses the IEEE classification to learn the maximum power consumption of a powered device before powering it. The switch grants power only when the maximum wattage configured on the port is less than or equal to the IEEE class maximum. This ensures that the switch power budget is not oversubscribed. There is no such mechanism in Cisco prestandard powered devices.

The workaround for networks with pre-standard powered devices is to leave the maximum wattage set at the default value (15.4 W). You can also configure the maximum wattage for the port for no less than the value the powered device reports as the power consumption through CDP messages. For networks with IEEE Class 0, 3, or 4 devices, do not configure the maximum wattage for the port at less than the default 15.4 W (15,400 milliwatts). (CSCee80668)

- Phone detection events that are generated by many IEEE phones connected to the switch ports can consume a significant amount of CPU time if the switch ports cannot power the phones because the internal link is down.

The workaround is to enter the **power inline never** interface configuration command on all the Fast Ethernet ports that are not powered by but are connected to IP phones if the problem persists. (CSCef84975, Cisco EtherSwitch service modules only)

- Some access point devices are incorrectly discovered as IEEE 802.3af Class 1 devices. These access points should be discovered as Cisco pre-standard devices. The **show power inline** user EXEC command shows the access point as an IEEE Class 1 device. The workaround is to power the access point by using an AC wall adaptor. (CSCin69533)
- The Cisco 7905 IP Phone is error-disabled when the phone is connected to wall power.

The workaround is to enable PoE and to configure the switch to recover from the PoE error-disabled state. (CSCsf32300)

MAC Addressing

This is the MAC addressing limitation:

(Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) When a MAC address is configured for filtering on the internal VLAN of a routed port, incoming packets from the MAC address to the routed port are not dropped. (CSCeb67937)

Management

CiscoWorks is not supported on the Catalyst 3750-24FS switch.

Multicasting

These are the multicasting limitations:

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The switch does not support tunnel interfaces for unicast routed traffic. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnel interfaces are supported for multicast routing.
- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) Nonreverse-path forwarded (RPF) IP multicast traffic to a group that is bridged in a VLAN is leaked onto a trunk port in the VLAN even if the port is not a member of the group in the VLAN, but it is a member of the group in another VLAN. Because unnecessary traffic is sent on the trunk port, it reduces the bandwidth of the port. There is no workaround for this problem because non-RPF traffic is continuous in certain topologies. As long as the trunk port is a member of the group in at least one VLAN, this problem occurs for the non-RPF traffic. (CSCdu25219)
- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise. The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)
- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port. There is no workaround. (CSCdy82818)
- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) When you use the **ip access-group** interface configuration command with a router access control list (ACL) to deny access to a group in a VLAN, multicast data to the group that is received in the VLAN is always flooded in the VLAN, regardless of IGMP group membership in the VLAN. This provides reachability to directly connected clients, if any, in the VLAN. The workaround is to not apply a router ACL set to deny access to a VLAN interface. Apply the security through other means; for example, apply VLAN maps to the VLAN instead of using a router ACL for the group. (CSCdz86110)
- (Catalyst 3750 switch stack) If the stack master is power cycled immediately after you enter the **ip mroute** global configuration command, there is a slight chance that this configuration change might be lost after the stack master changes. This occurs because the stack master did not have time to propagate the running configuration to all the stack members before it was powered down. This problem might also affect other configuration commands. There is no workaround. (CSCea71255)
- (Catalyst 3750 switches and Cisco EtherSwitch service modules) When you enable IP Protocol-Independent Multicast (PIM) on a tunnel interface, the switch incorrectly displays the `Multicast is not supported on tunnel interfaces` error message. IP PIM is not supported on tunnel interfaces. There is no workaround. (CSCeb75366)
- If an IGMP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
 - If the `ALLOW_NEW_SOURCE` record is before the `BLOCK_OLD_SOURCE` record, the switch removes the port from the group.

- If the `BLOCK_OLD_SOURCE` record is before the `ALLOW_NEW_SOURCE` record, the switch adds the port to the group.

There is no workaround. (CSCec20128)

- When IGMP snooping is disabled and you enter the **switchport block multicast** interface configuration command, IP multicast traffic is not blocked.

The **switchport block multicast** interface configuration command is only applicable to non-IP multicast traffic.

There is no workaround. (CSCee16865)

- Incomplete multicast traffic can be seen under either of these conditions:
 - You disable IP multicast routing or re-enable it globally on an interface.
 - A switch mroute table temporarily runs out of resources and recovers later.

The workaround is to enter the **clear ip mroute** privileged EXEC command on the interface. (CSCef42436)

After you configure a switch to join a multicast group by entering the **ip igmp join-group group-address** interface configuration command, the switch does not receive join packets from the client, and the switch port connected to the client is removed from the IGMP snooping forwarding table.

Use one of these workarounds:

- Cancel membership in the multicast group by using the **no ip igmp join-group group-address** interface configuration command on an SVI.
- Disable IGMP snooping on the VLAN interface by using the **no ip igmp snooping vlan vlan-id** global configuration command. (CSCeh90425)
- If IP routing is disabled and IP multicast routing is enabled on a switch running Cisco IOS Release 12.2(25)SED, IGMP snooping floods multicast packets to all ports in a VLAN.

The workaround is to enable IP routing or to disable multicast routing on the switch. You can also use the **ip igmp snooping querier** global configuration command if IP multicast routing is enabled for queries on a multicast router port. (CSCsc02995)

- A switch drops unicast traffic under these conditions:
 - The switch belongs to a Layer 2 ring.
 - More than 800 Mbps of multicast traffic is sent in both directions on the interface.

When multicast traffic is sent in one direction and unicast traffic is sent in another, unicast traffic is dropped at the multicast traffic source port.

The workaround is to apply a policy map so that the least significant traffic is discarded. (CSCsq83882)

Power

These are the powers limitation for the Cisco EtherSwitch service modules:

- Non-PoE devices attached to a network might be erroneously detected as an IEEE 802.3af-compliant powered device and powered by the Cisco EtherSwitch service module.

There is no workaround. You should use the **power inline never** interface configuration command on Cisco EtherSwitch service module ports that are not connected to PoE devices. (CSCee71979)

- When you enter the **show power inline** privileged EXEC command, the output shows the total power used by all Cisco EtherSwitch service modules in the router. The remaining power shown is available for allocation to switching ports on all Cisco EtherSwitch service modules in the router. To display the total power used by a specific EtherSwitch service module, enter the **show power inline** command on the router. This output appears:

```
Router# show power inline
PowerSupply  SlotNum.  Maximum  Allocated  Status
-----
INT-PS      0          360.000  121.000    PS1 GOOD  PS2 ABSENT
Interface   Config  Device  Powered  PowerAllocated
-----
Gi4/0      auto   Unknown On        121.000 Watts
```

This is not a problem because the display correctly shows the total used power and the remaining power available on the system. (CSCeg74337)

- Entering the **shutdown** and the **no shutdown** interface configuration commands on the internal link can disrupt the PoE operation. If a new IP phone is added while the internal link is in shutdown state, the IP phone does not get inline power if the internal link is brought up within 5 minutes.

The workaround is to enter the **shutdown** and the **no shutdown** interface configuration commands on the Fast Ethernet interface of a new IP phone that is attached to the service module port after the internal link is brought up. (CSCeh45465)

QoS

These are the quality of service (QoS) limitations:

- Some switch queues are disabled if the buffer size or threshold level is set too low with the **mls qos queue-set output** global configuration command. The ratio of buffer size to threshold level should be greater than 10 to avoid disabling the queue. The workaround is to choose compatible buffer sizes and threshold levels. (CSCea76893)
- When auto-QoS is enabled on the switch, priority queuing is not enabled. Instead, the switch uses shaped round robin (SRR) as the queuing mechanism. The auto-QoS feature is designed on each platform based on the feature set and hardware limitations, and the queuing mechanism supported on each platform might be different. There is no workaround. (CSCee22591)

Routing

These are the routing limitations:

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The switch does not support tunnel interfaces for unicast routed traffic. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnel interfaces are supported for multicast routing.
- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) A route map that has an ACL with a Differentiated Services Code Point (DSCP) clause cannot be applied to a Layer 3 interface. The switch rejects this configuration and displays a message that the route map is unsupported. There is no workaround. (CSCea52915)
- On a Catalyst 3750 or a Cisco EtherSwitch service module switch stack with a large number of switched virtual interfaces (SVIs), routes, or both on a fully populated nine-member switch stack, this message might appear when you reload the switch stack or add a switch to the stack:

```
%SYS-2-MALLOCFAIL: Memory allocation of 4252 bytes failed from 0x179C80, alignment 0
Pool: I/O Free: 77124 Cause: Memory fragmentation
Alternate Pool: None Free: 0 Cause: No Alternate pool
```

This error message means there is a temporary memory shortage that normally recovers by itself. You can verify that the switch stack has recovered by entering the **show cef line** user EXEC command and verifying that the line card states are `up` and `sync`. No workaround is required because the problem is self-correcting. (CSCea71611)

- (Catalyst 3750 switches and Cisco EtherSwitch service modules) A spanning-tree loop might occur if all of these conditions are true:
 - Port security is enabled with the violation mode set to protected.
 - The maximum number of secure addresses is less than the number of switches connected to the port.
 - There is a physical loop in the network through a switch whose MAC address has not been secured, and its BPDUs cause a secure violation.

The workaround is to change any one of the listed conditions. (CSCed53633)

SPAN and RSPAN

These are the SPAN and Remote SPAN (RSPAN) limitations.

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) An egress SPAN copy of routed unicast traffic might show an incorrect destination MAC address on both local and remote SPAN sessions. This limitation does not apply to bridged packets. The workaround for local SPAN is to use the **replicate** option. For a remote SPAN session, there is no workaround.

This is a hardware limitation and only applies to these switches (CSCdy72835):

- 3560-24PS
- 3560-48PS
- 3750-24PS
- 3750-48PS
- 3750-24TS
- 3750-48TS
- 3750G-12S
- 3750G-24T
- 3750G-24TS
- 3750G-16TD
- Cisco EtherSwitch service modules
- Egress SPAN routed packets (both unicast and multicast) show the incorrect source MAC address. For remote SPAN packets, the source MAC address should be the MAC address of the egress VLAN, but instead the packet shows the MAC address of the RSPAN VLAN. For local SPAN packets with native encapsulation on the destination port, the packet shows the MAC address of VLAN 1. This problem does not appear with local SPAN when the **encapsulation replicate** option is used. This limitation does not apply to bridged packets. The workaround is to use the **encapsulate replicate** keywords in the **monitor session** global configuration command. Otherwise, there is no workaround.

This is a hardware limitation and only applies to these switches (CSCdy81521):

- 3560-24PS
- 3560-48PS
- 3750-24PS
- 3750-48PS
- 3750-24TS

- 3750-48TS
- 3750G-12S
- 3750G-24T
- 3750G-24TS
- 3750G-16TD
- Cisco EtherSwitch service modules
- During periods of very high traffic when two RSPAN source sessions are configured, the VLAN ID of packets in one RSPAN session might overwrite the VLAN ID of the other RSPAN session. If this occurs, packets intended for one RSPAN VLAN are incorrectly sent to the other RSPAN VLAN. This problem does not affect RSPAN destination sessions. The workaround is to configure only one RSPAN source session.

This is a hardware limitation and only applies to these switches (CSCea72326):

- 3560-24PS
- 3560-48PS
- 3750-24PS
- 3750-48PS
- 3750-24TS
- 3750-48TS
- 3750G-12S
- 3750G-24T
- 3750G-24TS
- 3750G-16TD
- Cisco EtherSwitch service modules
- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The egress SPAN data rate might degrade when fallback bridging or multicast routing is enabled. The amount of degradation depends on the processor loading. Typically, the switch can egress SPAN at up to 40,000 packets per second (64-byte packets). As long as the total traffic being monitored is below this limit, there is no degradation. However, if the traffic being monitored exceeds the limit, only a portion of the source stream is spanned. When this occurs, the following console message appears: `Decreased egress SPAN rate`. In all cases, normal traffic is not affected; the degradation limits only how much of the original source stream can be egress spanned. If fallback bridging and multicast routing are disabled, egress SPAN is not degraded. There is no workaround. If possible, disable fallback bridging and multicast routing. If possible, use ingress SPAN to observe the same traffic. (CSCeb01216)
- On Catalyst 3750 switches running Cisco IOS Release 12.1(14)EA1 and later, on Catalyst 3560 switches running Cisco IOS release 12.1(19)EA1 or later, or on Cisco EtherSwitch service modules, some IGMP report and query packets with IP options might not be ingress-spanned. Packets that are susceptible to this problem are IGMP packets containing 4 bytes of IP options (IP header length of 24). An example of such packets would be IGMP reports and queries having the router alert IP option. Ingress-spanning of such packets is not accurate and can vary with the traffic rate. Typically, very few or none of these packets are spanned. There is no workaround. (CSCeb23352)

- Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session. The workaround is to use the **monitor session *session_number* destination {interface *interface-id* encapsulation replicate}** global configuration command for local SPAN. (CSCed24036)

Stacking (Catalyst 3750 or Cisco EtherSwitch service module switch stack only)

These are the Catalyst 3750 and Cisco EtherSwitch service module switch stack limitations:

- If the stack master is immediately reloaded after adding multiple VLANs, the new stack master might fail. The workaround is to wait a few minutes after adding VLANs before reloading the stack master. (CSCea26207)
- If the console speed is changed on a stack, the configuration file is updated, but the baud rate is not. When the switch is reloaded, meaningless characters might appear on the console during bootup before the configuration file is parsed and the console speed is set to the correct value. If manual bootup is enabled or the startup configuration is deleted after you change the console speed, you cannot access the console after the switch reboots. There is no workaround. (CSCec36644)
- If a switch is forwarding traffic from a Gigabit ingress interface to a 100 Mb/s egress interface, the ingress interface might drop more packets due to oversubscription if the egress interface is on a Fast Ethernet switch (such as a Catalyst 3750-24TS or 3750-48TS switch) than if it is on a Gigabit Ethernet switch (such as a Catalyst 3750G-24T or 3750G-24TS switch). There is no workaround. (CSCed00328)
- If a stack member is removed from a stack and either the configuration is not saved or another switch is added to the stack at the same time, the configuration of the first member switch might be lost. The workaround is to save the stack configuration before removing or replacing any switch in the stack. (CSCed15939)
- When the **switchport** and **no switchport** interface configuration commands are entered more than 20,000 times on a port of a Catalyst 3750 switch or on a Cisco EtherSwitch service module, all available memory is used, and the switch halts.
There is no workaround. (CSCed54150)
- In a private-VLAN domain, only the default private-VLAN IP gateways have sticky ARP enabled. The intermediate Layer 2 switches that have private VLAN enabled disable sticky ARP. When a stack master re-election occurs on one of the Catalyst 3750 or Cisco EtherSwitch service module default IP gateways, the message `IP-3-STCKYARPOVR` appears on the consoles of other default IP gateways. Because sticky ARP is not disabled, the MAC address update caused by the stack master re-election cannot complete.
The workaround is to complete the MAC address update by entering the **clear arp** privileged EXEC command. (CSCed62409)
- When a Catalyst 3750 switch or Cisco EtherSwitch service module is being reloaded in a switch stack, packet loss might occur for up to 1 minute while the Cisco Express Forwarding (CEF) table is downloaded to the switch. This only impacts traffic that will be routed through the switch that is being reloaded. There is no workaround. (CSCed70894)

- Inconsistent private-VLAN configuration can occur on a switch stack if a new stack master is running the IP base image (formerly known as the SMI) and the old stack master was running the IP services image (formerly known as the EMI).

Private VLAN is enabled or disabled on a switch stack, depending on whether or not the stack master is running the IP services image (formerly known as the EMI) or the IP base image (formerly known as the SMI):

- If the stack master is running the IP services image (formerly known as the EMI), all stack members have private VLAN enabled.
- If the stack master is running the IP base image (formerly known as the SMI), all stack members have private VLAN disabled.

This occurs after a stack master re-election when the previous stack master was running the IP services image (formerly known as the EMI) and the new stack master is running the IP base image (formerly known as the SMI). The stack members are configured with private VLAN, but any new switch that joins the stack will have private VLAN disabled.

These are the workarounds. Only one of these is necessary:

- Reload the stack after an IP services image (formerly known as the EMI) to IP base image (formerly known as the SMI) master switch change (or the reverse).
 - Before an IP services image (formerly known as the EMI)-to-IP base image (formerly known as the SMI) master switch change, delete the private-VLAN configuration from the existing stack master. (CSCee06802)
- Port configuration information is lost when changing from **switchport** to **no switchport** modes on Catalyst 3750 switches.

This is the expected behavior of the offline configuration (provisioning) feature. There is no workaround. (CSCee12431)

- If one switch in a stack of Catalyst 3750 switches requires more time than the other switches to find a bootable image, it might miss the stack master election window. However, even if the switch does not participate in the stack master election, it will join the stack as a member.

The workaround is to copy the bootable image to the parent directory or first directory. (CSCei69329)

- When the path cost to the root bridge is equal from a port on a stacked root and a port on a non stack root, the BLK port is not chosen correctly in the stack when the designated bridge priority changes. This problem appears on switches running in PVST, Rapid-PVST, and MST modes.

The workaround is to assign a lower path cost to the forwarding port. (CSCsd95246)

- When a stack of 3750 switches is configured with a Cross-Stack EtherChannel and one of the physical ports in the EtherChannel has a link-up or a link-down event, the stack might transmit duplicate packets across the EtherChannel. The problem occurs during the very brief interval while the switch stack is adjusting the EtherChannel for changing conditions and adapting the load balance algorithm to the new set of active physical ports.

This can but does not always occur during link flaps and does not last for more than a few milliseconds. This problem can happen for cross-stack EtherChannels with the mode set to ON or LACP.

There is no workaround. No manual intervention is needed. The problem corrects itself within a short interval after the link flap as all the switches in the stack synchronize with the new load-balance configuration. (CSCse75508)

- If a new member switch joins a switch stack within 30 seconds of a command to copy the switch configuration to the running configuration of the stack master being entered, the new member might not get the latest running configuration and might not operate properly.

The workaround is to reboot the new member switch. Use the **remote command all show run** privileged EXEC command to compare the running configurations of the stack members. (CSCsf31301)

- The error message `DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND` might appear for a switch stack under these conditions:
 - IEEE 802.1 is enabled.
 - A supplicant is authenticated on at least one port.
 - A new member joins a switch stack.

You can use one of these workarounds:

- Enter the **shutdown** and the **no shutdown** interface configuration commands to reset the port.
- Remove and reconfigure the VLAN. (CSCsi26444)
- In a mixed stack of Catalyst 3750 switches and Catalyst 3750-E switches, when the stack reloads, the Catalyst 3750-E might not become stack master, even it has a higher switch priority set.

The workaround is to check the flash. If it contains many files, remove the unnecessary ones. Check the lost and found directory in flash and if there are many files, delete them. To check the number of files use the **fsck flash:** command. (CSCsi69447)

- After a stack bootup, the spanning tree state of a port that has IEEE 802.1x enabled might be blocked, even when the port is in the authenticated state. This can occur on a voice port where the Port Fast feature is enabled.

The workaround is to enter a **shutdown** interface configuration command followed by a **no shutdown** command on the port in the blocked state. (CSCsl64124)

Trunking

These are the trunking limitations:

- The switch treats frames received with mixed encapsulation (IEEE 802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and the port LED blinks amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an IEEE 802.1Q trunk interface. There is no workaround. (CSCdz33708)
- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y. There is no workaround. (CSCdz42909).
- If a Catalyst 3750 switch stack is connected to a designated bridge and the root port of the switch stack is on a different switch than the alternate root port, changing the port priority of the designated ports on the designated bridge has no effect on the root port selection for the Catalyst 3750 switch stack. There is no workaround. (CSCea40988)

- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics. There is no workaround. (CSCec35100).

VLAN

These are the VLAN limitations:

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.

The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)

- (Catalyst 3750 or 3560 switches) A CPUHOG message sometimes appears when you configure a private VLAN. Enable port security on one or more of the ports affected by the private VLAN configuration.

There is no workaround. (CSCed71422)

- (Catalyst 3750) When you apply a per-VLAN quality of service (QoS), per-port policer policy-map to a VLAN Switched Virtual Interface (SVI), the second-level (child) policy-map in use cannot be re-used by another policy-map.

The workaround is to define another policy-map name for the second-level policy-map with the same configuration to be used for another policy-map. (CSCef47377)

- When dynamic ARP inspection is configured on a VLAN, and the ARP traffic on a port in the VLAN is within the configured rate limit, the port might go into an error-disabled state.

The workaround is to configure the burst interval to more than 1 second. (CSCse06827, Catalyst 3750 switches only)

- When line rate traffic is passing through a dynamic port, and you enter the **switchport access vlan dynamic** interface configuration command for a range of ports, the VLANs might not be assigned correctly. One or more VLANs with a null ID appears in the MAC address table instead.

The workaround is to enter the **switchport access vlan dynamic** interface configuration command separately on each port. (CSCsi26392)

Device Manager Limitations

These are the device manager limitations:

- When you are prompted to accept the security certificate and you click *No*, you only see a blank screen, and the device manager does not launch.

The workaround is to click *Yes* when you are prompted to accept the certificate. (CSCef45718)

Important Notes

These sections describe the important notes related to this software release for the Catalyst 3750, 3560, and 2960 switches and for the Cisco EtherSwitch service modules:

- [Switch Stack Notes, page 35](#)
- [Cisco IOS Notes, page 35](#)
- [Device Manager Notes, page 36](#)

Switch Stack Notes

These notes apply to switch stacks:

- Always power off a switch before adding or removing it from a switch stack.
- Catalyst 3560 switches do not support switch stacking. However, the **show processes** privileged EXEC command still lists stack-related processes. This occurs because these switches share common code with other switches that do support stacking.
- Catalyst 3750 switches running Cisco IOS Release 12.2(25)SEB are compatible with Cisco EtherSwitch service modules running Cisco IOS Release 12.2(25)EZ. Catalyst 3750 switches and Cisco EtherSwitch service modules can be in the same switch stack. In this switch stack, the Catalyst 3750 switch or the Cisco EtherSwitch service module can be the stack's active switch.

Cisco IOS Notes

These notes apply to Cisco IOS software:

- The Catalyst 2960-48PST-L, 2960-8TC-S, and 2960-48TT-S switches support up to 208 IGMP groups. The other Catalyst 2960 switches support up to 250 IGMP groups.
- The IEEE 802.1x feature in Cisco IOS Release 12.1(14)EA1 and later is not fully backward-compatible with the same feature in Cisco IOS Release 12.1(11)AX. If you are upgrading a Catalyst 3750 switch running Cisco IOS Release 12.1(11)AX that has IEEE 802.1x configured, you must re-enable IEEE 802.1x after the upgrade by using the **dot1x system-auth-control** global configuration command. This global command does not exist in Cisco IOS Release 12.1(11)AX. Failure to re-enable IEEE 802.1x weakens security because some hosts can then access the network without authentication.
- The behavior of the **no logging on** global configuration command changed in Cisco IOS Release 12.2(18)SE and later. In Cisco IOS Release 12.1(19)EA and earlier, both of these command pairs disabled logging to the console:
 - the **no logging on** and then the **no logging console** global configuration commands
 - the **logging on** and then the **no logging console** global configuration commands

In Cisco IOS Release 12.2(18)SE and later, you can only use the **logging on** and then the **no logging console** global configuration commands to disable logging to the console. (CSCec71490)

- In Cisco IOS Release 12.2(25)SEC for the Catalyst 3750 and 3560 switches and in Cisco IOS Release 12.2(25)SED for the Catalyst 2960 switch, the implementation for multiple spanning tree (MST) changed from the previous release. Multiple STP (MSTP) complies with the IEEE 802.1s standard. Previous MSTP implementations were based on a draft of the IEEE 802.1s standard.

- If the switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

```
00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not responding.
```

If this message appears, check that there is network connectivity between the switch and the ACS. You should also check that the switch has been properly configured as an AAA client on the ACS.

- If the switch has interfaces with automatic QoS for voice over IP (VoIP) configured and you upgrade the switch software to Cisco IOS Release 12.2(40)SE (or later), when you enter the **auto qos voip cisco-phone** interface configuration command on another interface, you might see this message:

```
AutoQoS Error: ciscophone input service policy was not properly applied
policy map AutoQoS-Police-CiscoPhone not configured
```

If this happens, enter the **no auto qos voip cisco-phone** interface command on all interface with this configuration to delete it. Then enter the **auto qos voip cisco-phone** command on each of these interfaces to reapply the configuration.

Device Manager Notes

These notes apply to the device manager:

- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or Cisco Network Assistant.
- When the switch is running a localized version of the device manager, the switch displays settings and status only in English letters. Input entries on the switch can only be in English letters.
- For device manager session on Internet Explorer, popup messages in Japanese or in simplified Chinese can appear as garbled text. These messages appear properly if your operating system is in Japanese or Chinese.
- The Legend on the device manager incorrectly includes the 1000BASE-BX SFP module.
- We recommend this browser setting to speed up the time needed to display the device manager from Microsoft Internet Explorer.

From Microsoft Internet Explorer:

1. Choose **Tools > Internet Options**.
 2. Click **Settings** in the “Temporary Internet files” area.
 3. From the Settings window, choose **Automatically**.
 4. Click **OK**.
 5. Click **OK** to exit the Internet Options window.
- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip http authentication {aaa enable local}	Configure the HTTP server interface for the type of authentication that you want to use. <ul style="list-style-type: none"> • aaa—Enable the authentication, authorization, and accounting feature. You must enter the aaa new-model interface configuration command for the aaa keyword to appear. • enable—Enable password, which is the default method of HTTP server user authentication, is used. • local—Local user database, as defined on the Cisco router or access server, is used.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.

- The device manager uses the HTTP protocol (the default is port 80) and the default method of authentication (the enable password) to communicate with the switch through any of its Ethernet ports and to allow switch management from a standard web browser.

If you change the HTTP port, you must include the new port number when you enter the IP address in the browser **Location** or **Address** field (for example, <http://10.1.126.45:184> where 184 is the new HTTP port number). You should write down the port number through which you are connected. Use care when changing the switch IP information.

If you are *not* using the default method of authentication (the enable password), you need to configure the HTTP server interface with the method of authentication used on the switch.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip http authentication {enable local tacacs}	Configure the HTTP server interface for the type of authentication that you want to use. <ul style="list-style-type: none"> • enable—Enable password, which is the default method of HTTP server user authentication, is used. • local—Local user database, as defined on the Cisco router or access server, is used. • tacacs—TACACS server is used.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.

- If you use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, www.cisco.com:84), you must enter *http://* as the URL prefix. Otherwise, you cannot launch the device manager.

Open Caveats

This section describes the open caveats with possible unexpected activity in this software release. Unless otherwise noted, these severity 3 Cisco IOS configuration caveats apply to the Catalyst 3750, 3560, and 2960 switches and to Cisco EtherSwitch service modules:

- CSCeh01250 (Cisco EtherSwitch service modules)

When connected to the router through an auxiliary port in a session to a Cisco EtherSwitch service module, the service module session fails when you enter the **shutdown** and the **no shutdown** interface configuration commands on the service module router interface.

These are the workarounds:

- Reload the router.
- Connect to the router through the console port, and open a session to the service module.

- CSCeh35595 (Cisco EtherSwitch service modules)

A duplex mismatch occurs when two Fast Ethernet interfaces that are directly connected on two EtherSwitch service modules are configured as both 100 Mb/s and full duplex *and* as automatic speed and duplex settings. This is expected behavior for the PHY on the Cisco EtherSwitch service modules.

There is no workaround.

- CSCeh52964 (Cisco EtherSwitch service modules)

When the router is rebooted after it is powered on (approximately once in 10 to 15 reboots), the Router Blade Communication Protocol (RBCP) between the router and the EtherSwitch service module might not be reestablished, and this message appears:

```
[date]: %Y88E8K-3-ILP_MSG_TIMEOUT_ERROR: GigabitEthernet1/0: EtherSwitch Service
Module RBCP ILP messages timeout
```

The workaround is to reload the EtherSwitch service module software without rebooting the router. You can reload the switching software by using the **reload** user EXEC command at the EtherSwitch service module prompt or by using the **service-module g slot_numer /0 reset** privileged EXEC command at the router prompt.

- CSCsk65142

When you enter the **boot host retry timeout** global configuration command to specify the amount of time that the client should keep trying to download the configuration and you do not enter a timeout value, the default value is zero, which should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.

The workaround is to always enter a non zero value for the timeout value when you enter the **boot host retry timeout timeout-value** command.

- CSCsk96058 (Catalyst 3750 switches)

A stack member switch might fail to bundle Layer 2 protocol tunnel ports into a port channel when you have followed these steps:

1. You configure a Layer 2 protocol tunnel port on the master switch.
2. You configure a Layer 2 protocol tunnel port on the member switch.
3. You add the port channel to the Layer 2 protocol tunnel port on the master switch.
4. You add the port channel to the Layer 2 protocol tunnel port on the member switch.

After this sequence of steps, the member port might stay suspended.

The workaround is to configure the port on the member switch as a Layer 2 protocol tunnel and at the same time also as a port channel. For example:

```
Switch(config)# interface fastethernet1/0/11
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# channel-group 1 mode on
```

- CSCsl02680 (Catalyst 3750 and 3560 switches)

When the configuration file is removed from the switch and the switch is rebooted, port status for VLAN 1 and the management port (Fast Ethernet 0) is sometimes reported as `up` and sometimes as `down`, resulting in conflicts. This status depends on when you respond to the reboot query:

Would you like to enter the initial configuration dialog?

- After a reboot if you wait until the Line Protocol status of VLAN 1 appears on the console before responding, VLAN 1 line status is always shown as `down`. This is the correct state.
- The problem (VLAN 1 reporting `up`) occurs if you respond to the query before VLAN 1 line status appears on the console.

The workaround is to wait for approximately 1 minute after rebooting and until the VLAN 1 interface line status appears on the console before you respond to the query.

- CSCso96778

When you use the **ipv6 address dhcp** interface configuration command on an interface that is configured in router mode, other addresses on the prefix associated with the new address might not be accessible.

The workaround is to use the **ipv6 address dhcp** interface configuration command on an interface that is configured in host mode, or configure a static route to the prefix through the interface.

- CSCsr53843 (Catalyst 3750-48PS switches)

When a stack member is connected to another switch through an uplink, the remote switch might prune the member VLAN because there is no VTP join message from the stack member.

These are the workarounds:

- Move the uplink to the master switch in the switch stack.
- Disable VTP pruning globally or on the interface.
- Change the VLAN root to another switch.

- CSCsr65689

When loopback interfaces are configured, this error message might appear when a stack member is loading:

```
%COMMON_FIB-3-FIBIDBINCONS2
```

No workaround is required. This does not affect switch functionality.

- CSCsr79279 (Catalyst 2960 switches)

When disconnecting the Rx cable from a 1000BASE-X SFP module connected between a Catalyst 4000 Supervisor Engine IV and a Catalyst 2960 switch, the Catalyst 2960 switch does not detect linkdown, the status remains `up`. The Catalyst 4000 correctly detects link down.

There is no workaround.

Resolved Caveats

These are the caveats that have been resolved in this release. Unless otherwise noted, these resolved caveats apply to the Catalyst 3750, 3560, and 2960 switches and the Cisco EtherSwitch service modules.

- CSCin91851, CSCsh42013, and CSCsh42316

The SSH Protocol now supports generic message authentication and is compliant with RFC 4256.

- CSCsa73179 (Catalyst 3750 and 3560 switches)

A switch no longer fails under these conditions:

- A switch no longer fails under these conditions:
- OSPF is in the switch image.
- You enter the RIP **no default-information** router configuration command.

- CSCsc96474

These traceback messages such as these no longer appear when a large number of IEEE 802.1x supplicants repeatedly try to log in and log out.

```
Jan 3 17:54:32 L3A3 307: Jan 3 18:04:13.459: %SM-4-BADEVENT: Event 'eapReq' is invalid
for the current state 'auth_bend_idle': dot1x_auth_bend Fa9
Jan 3 17:54:32 L3A3 308: -Traceback= B37A84 18DAB0 2FF6C0 2FF260 8F2B64 8E912C Jan 3
19:06:13 L3A3 309: Jan 3 19:15:54.720: %SM-4-BADEVENT: Event 'eapReq_no_reAuthMax' is
invalid for the current ate 'auth_restart': dot1x_auth Fa4
```

- CSCsd03580

When IEEE 802.1x is globally disabled on the switch by using the **no dot1x system-auth-control** global configuration command, interface level IEEE 802.1x configuration commands, including the **dot1x timeout** and **dot1x mac-auth-bypass** commands, are now available.

- CSCse07265 (Catalyst 3750 and 3560 switches)

If you configure IP SLA to generate a syslog message for a reaction trap and an operation with a trigger of *timeout* or *connectionless*, a syslog message now appears when triggered.

- CSCsi70454

The configuration file used for the configuration replacement feature no longer requires the character string *end* at the end of the file.

- CSCsi71768 (Catalyst 3750 and 3560 switches)

If you upgrade the software image from Cisco IOS Release 12.2(25)SEE2 to Cisco IOS Release 12.2(35)SE1, the IPv6 static routes are now saved in the routing table.

- CSCsj74022 (Cisco EtherSwitch service modules)

The switch now correctly updates the entPhysicalChildIndex objects from the ENTITY-MIB, and all of the entPhysicalChildIndex entries appear in the table.

- CSCsj87991

A switch configured for Link Layer Discovery Protocol (LLDP) now correctly reports the enabled switch capabilities in the LLDP type, length, and value (TLV) attributes. System capabilities appear correctly, and the enabled capabilities are now identified if the switch is configured only as a Layer 2 switch.

- CSCsj10198 (Catalyst 3750 and 3560 switches)
When a per-port per-VLAN policy map (a hierarchical VLAN-based policy map) is attached to a VLAN interface and you remove the child-policy policer from the policy map and then restore it, the policy map now correctly re-attaches to the same SVI.
- CSCsk09459 (Catalyst 3750 switches)
When a switch stack boots up, traceback messages no longer appear on the console when the switch stack has 400 or more VLANs and multicast or port-security features.
- CSCsk47893 (Catalyst 3750 and 3560 switches)
A switch running the IP base image now supports full EIGRP stub routing.
- CSCsk53850 (Catalyst 3750 switches)
If you enter the **no ip vrf vrf-name** global configuration command to delete a VPN routing/forwarding instance on the switch when routing is not enabled on the switch, the VRF instance is no longer held in the delete queue. The VRF entry does not appear in the output when you enter the **show running-config** privileged EXEC command, and it no longer appears when you enter the **show ip vrf** privileged EXEC command.
- CSCsl72968 (Catalyst 3750 switches)
When multidomain authentication (MDA) is configured on a stack member, a switch port in that stack is no longer intermittently enter disabled when the stack reloads.
- CSCsm12766 (Catalyst 3750 switches)
The **vlan dot1q tag native** global configuration command now works correctly.
- CSCsm88601
When multiple voice-over-IP phones are connected to a switch or switch stack with MAC authentication bypass enabled, setting the IEEE 802.1x timeout period too low no longer can cause a switch in single-host mode to authenticate the phones using MAC authentication bypass, except when other data packets are received before CDP packets.
- CSCso22855 (Catalyst 3750 and 3560 switches, Catalyst 2960 switches running the IP base image)
If you specify the router ID before entering the **autonomous-system autonomous-system-number** address-family configuration command, the router ID is no longer lost when the switch reloads.
- CSCso22883 (Catalyst 3750 and 3560 switches, Catalyst 2960 switches running the IP base image)
Any form of the **passive-interface** command entered in one instance propagates to all configured address-family instances for the same EIGRP routing process.
- CSCso23165
When the **ip pim sparse-mode** and **ip wccp web-cache redirect in** configuration commands are applied on a global table interface, traffic is now sent to multicast receivers.
- CSCso40282 (Catalyst 3750 switches)
A switch stack no longer stops sending CDP packets when more than 100 IP phones are connected to the stack.
- CSCso54866 (Catalyst 3750 switches)
Outgoing packets are no longer dropped from an interface with policy-based routing (PBR):
 - Any static route is configured with a next-hop IP-address that is the same as the PBR next-hop address.
 - Address Resolution Protocol (ARP) for the next-hop is incomplete.

- CSCso70893 (Catalyst 3750 switches)

A message similar to this one no longer appears when you log into a switch through an SSH session and upgrade the switch by using the **archive download-sw** privileged EXEC command

```
*Mar 11 06:48:22.729 JST: %SCHED-3-THRASHING: Process thrashing on watched message
event. -Process= "SSH Process", ipl= 6, pid= 147
```

- CSCso72052 (Catalyst 3750 and 3560 switches)

An end host no longer remains in the guest VLAN after IEEE 802.1X authentication.

- CSCso81660 (Catalyst 3750 switches)

The **show interfaces** command output for a switch stack now shows the correct values for the output drops.

- CSCsq17094 (Catalyst 3750 switches)

Downstream switch interfaces in a link state group no longer fail under these conditions:

- The switch is part of a stack.
- There is a master switch over.
- Some (or all) of the link state group interfaces are on the switch that becomes the new stack master.

- CSCsq27267 (Catalyst 3750 switches)

A switch stack now sends VTP join message for a VLAN interface without access ports associated with it.

- CSCsq38082

The cluster configuration is now saved to each cluster member when you save the configuration to the cluster commander.

- CSCsq86527 (Catalyst 3560 switches)

The Catalyst 3560 switch-management port LED now works as described in Figure 1-8 of the hardware installation guide:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3750e_3560e/hardware/installation/guide/HIGOVERV.html#wp1228781

- CSCsr50978 (Catalyst 3750 switches)

An EtherChannel with ports across stack members and configured to tunnel Layer 2 protocol packets (using the **l2protocol-tunnel** interface configuration command), no longer drops protocol packets received on a switch in the EtherChannel that is not the stack master.

- CSCsr55949

When IEEE 802.1x is enabled on the switch, EAP notification packets are no longer dropped.

Documentation Updates

This section provides these updates to the product documentation for the Catalyst 3750, 3560, and 2960 switches:

- [Updates to the Software Configuration Guides, page 43](#)
- [Updates to Only the Catalyst 3750 and 3560 Switch Software Configuration Guides, page 44](#)
- [Updates to the System Message Guides, page 45](#)
- [Updates to the Catalyst 3750, 3560, and 2960 Hardware Installation Guide, page 50](#)
- [Update to the Regulatory Compliance and Safety Information for the Catalyst 2960 Switch, page 51](#)
- [Updates to the Catalyst 3750 Getting Started Guide, page 52](#)
- [Updates to the Regulatory Compliance and Safety Information for the Catalyst 3750 Switch, page 56](#)

Updates to the Software Configuration Guides

This section is added to the “Configuring IPv4 ACLs” section in the “Configuring Network Security with ACLs” chapter.

Troubleshooting ACLS

If this access control list (ACL) manager message appears and [chars] is the access-list name,

```
ACLNGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

The switch has insufficient resources to create a hardware representation of the ACL. The resources include hardware memory and label space but not CPU memory. A lack of available logical operation units or specialized hardware resources causes this problem. Logical operation units are needed for a TCP flag match or a test other than **eq** (**ne**, **gt**, **lt**, or **range**) on TCP, UDP, or SCTP port numbers.

Use one of these workarounds:

- Modify the ACL configuration to use fewer resources.
- Rename the ACL with a name or number that alphanumerically precedes the ACL names or numbers.

To determine the specialized hardware resources, enter the **show platform layer4 acl map** privileged EXEC command. If the switch does not have available resources, the output shows that index 0 to index 15 are not available.

For more information about configuring ACLs with insufficient resources, see CSCsq63926 in the Bug Toolkit.

For example, if you apply this ACL to an interface:

```
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
permit tcp source source-wildcard destination destination-wildcard
```

And if this message appears:

```
ACLNGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

The flag-related operators are not available. To avoid this issue,

- Move the fourth ACE before the first ACE by using **ip access-list resequence** global configuration command:

```
permit tcp source source-wildcard destination destination-wildcard
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
```

or

- Rename the ACL with a name or number that alphanumerically precedes the other ACLs (for example, rename ACL 79 to ACL 1).

You can now apply the first ACE in the ACL to the interface. The switch allocates the ACE to available mapping bits in the Opselect index and then allocates flag-related operators to use the same bits in the TCAM.

Updates to Only the Catalyst 3750 and 3560 Switch Software Configuration Guides

These are updates for only the 3750 and 3560 software configuration guides:

- If the switch is running the IP base image, you can configure complete EIGRP routing. However, the configuration is not implemented because the IP base image supports only EIGRP stub routing, as described in the “Configuring IP Unicast Routing” chapter of the software configuration guide.

After you have entered the **eigrp stub** router configuration command, only the **eigrp stub connected summary** command takes effect. Although the CLI help might show the **receive-only** and **static** keywords and the you can enter these keywords, the switch running the IP base image always behaves as if the **connected** and **summary** keywords were configured.

- In the “Multi-VRF CE Configuration Guidelines” section of the “Configuring IP Unicast Routing” chapter of the *Catalyst 3750 Switch Software Configuration Guide* and the *Catalyst 3560 Switch Software Configuration Guide*, this guideline is incorrect:

If no VRFs are configured, 104 policies can be configured.

This is the correct guideline:

If no VRFs are configured, up to 105 policies can be configured.

- This information is added to the “Using IEEE 802.1x Authentication with Per-User ACLs” section of “Configuring IEEE 802.1x Port-Based Authentication” chapter of the software configuration guide:

Per-user ACLs are supported only in single-host mode.

- In the “Configuration Guidelines” section of the “Configuring Flex Links and the MAC Address-Table Move Update Feature” chapter, this guideline is added:

You can configure up to 16 backup links.

- This information is added to the “Using Route Maps to Redistribute Routing Information” section in the “Configuring IP Unicast Routing” chapter of the software configuration guide:



Note

A route map with no **set** route-map configuration commands is sent to the CPU, which causes high CPU utilization.

- These guidelines are added to the "Port Security Configuration Guidelines" in the "Configuring Port-Based Traffic Control" chapter:

When a trunk port configured with port security and assigned to an access VLAN for data traffic and to a voice VLAN for voice traffic, entering the **switchport voice** and **switchport priority extend** interface configuration commands has no effect.

When a connected device uses the same MAC address to request an IP address for the access VLAN and then an IP address for the voice VLAN, only the access VLAN is assigned an IP address.

- Unsupported Embedded Event Manager commands

Privileged EXEC:

- **event manager scheduler clear**
- **event manager update user policy**
- **show event manager detector**
- **show event manager version**

Global configuration:

- **event manager detector rpc**
- **event manager directory user repository**

Applet configuration (config-applet) :

- **event rpc**
- **event snmp-notification**
- **trigger (EEM)**

Trigger applet configuration (config-applet-trigger):

- **attribute (EEM)**
- **correlate**

Event trigger configuration (config-event-trigger) :

- **event owner**

Updates to the System Message Guides

This section contains the system message guide updates.

New System Messages

These messages were added to all of the system message guides:

Error Message ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]

Explanation There are insufficient resources available to create a hardware representation of the ACL. A lack of available logical operation units or specialized hardware resources can cause this problem. Logical operation units are needed for a TCP flag match or a test other than **eq** (**ne**, **gt**, **lt**, or **range**) on TCP, UDP, or SCTP port numbers.

Recommended Action Modify the ACL configuration to use fewer resources, or rename the ACL with a name or number that alphanumerically precedes the other ACL names or numbers.

Error Message ACLMGR-3-INVALIDPARAM: Invalid [chars] [int] encountered

Explanation The access control list (ACL) manager has encountered an invalid parameter value. [chars] is the parameter name, and [int] is the parameter value.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the “Error Message Traceback Reports” section.

Error Message DOT1X_SWITCH-5-ERR_ADDING_ADDRESS: Unable to add address [enet] on [chars]

Explanation The client MAC address could not be added to the MAC address table because the hardware memory is full or the address is a secure address on another port. [enet] is the supplicant MAC address, and [chars] is the interface. This message might appear if the IEEE 802.1x feature is enabled.

Recommended Action If the hardware memory is full, remove some of the dynamic MAC addresses. If the client address is on another port, manually remove it from that port.

Error Message PAGP_DUAL_ACTIVE-3-OBJECT_CREATE_FAILED: Unable to create [chars]

Explanation The switch cannot create the specified managed object. [chars] is the object name.

Recommended Action No action is required.

Error Message %PAGP_DUAL_ACTIVE-3-RECOVERY_TRIGGER: PAgP running on [chars] informing virtual switches of dual-active: new active id [enet], old id [enet]

Explanation Port Aggregation Protocol (PAgP) received a new active ID on the specified interface, which means that all virtual switches are in a dual-active scenario. The interface is informing virtual switches of this, which causes one switch to go into recovery mode. [chars] is the interface. The first [enet] is the new active ID. The second [enet] is the ID that it replaces.

Recommended Action No action is required.

Error Message %PAGP_DUAL_ACTIVE-3-REGISTRY_ADD_ERR: Failure in adding to [chars] registry

Explanation The switch could not add a function to the registry. [chars] is the registry name.

Recommended Action No action is required.

Error Message PLATFORM_HCEF-3-ADJ: [chars]

Explanation This message appears when an unsupported feature is configured on a switch running Cisco IOS Release 12.2(25)SE. [chars] is the error message.

Recommended Action Determine if a generic routing encapsulation (GRE) tunnel or the **ip cef accounting** global configuration command are configured. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnels are supported. If the GRE tunnel is configured, remove the tunnel, or upgrade the switch software to a Cisco IOS release when the GRE feature is needed. If the **ip cef accounting** command is configured, remove it by using the **no ip cef accounting** global configuration command.



Note

Cisco IOS Release 12.2(25)SEB2 does not support the **ip cef accounting** command.

Error Message PLATFORM_IPv6_UCAST-6-PREFIX: One or more, more specific prefixes could not be programmed into TCAM and are being covered by a less specific prefix

Explanation A more specific prefix could not be programmed into Ternary Content Addressable Memory (TCAM) and is covered by a less specific prefix. This could be a temporary condition. The output of the **show platform ipv6 unicast retry route** privileged EXEC command lists the failed prefixes.

Recommended Action No action is required.

Error Message PLATFORM_UCAST-6-PREFIX: One or more, more specific prefixes could not be programmed into TCAM and are being covered by a less specific prefix

Explanation A more specific prefix could not be programmed into Ternary Content Addressable Memory (TCAM) and is covered by a less specific prefix. This could be a temporary condition. The output of the **show platform ip unicast failed route** privileged EXEC command lists the failed prefixes.

Recommended Action No action is required.

Error Message %PM-6-EXT_VLAN_ADDITION: Extended VLAN is not allowed to be configured in VTP CLIENT mode.

Explanation The switch did not add a VLAN in VTP client mode.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the “Error Message Traceback Reports” section in the system message guides.

Error Message SPANTREE-6-PORTADD_ALL_VLANS: [chars] added to all Vlans

Explanation The interface has been added to all VLANs. [chars] is the added interface.

Recommended Action No action is required.

Error Message SPANTREE-6-PORTDEL_ALL_VLANS: [chars] deleted from all Vlans

Explanation The interface has been deleted from all VLANs. [chars] is the deleted interface.

Recommended Action No action is required.

Error Message SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to [chars].

Explanation The VLAN Trunking Protocol (VTP) domain name was changed through the configuration to the name specified in the message. [chars] is the changed domain name.

Recommended Action No action is required.

These messages were added to the Catalyst 3750 and 3560 system message guides:

Error Message VQPCCLIENT-2-TOOMANY: Interface [chars] shutdown by active host limit.

Explanation The system has shut down the specified interface because too many hosts have requested access to that interface. [chars] is the interface name.

Recommended Action To enable the interface, remove the excess hosts, and enter the **no shutdown** interface configuration command.

Error Message VQPCCLIENT-3-VLANNAME: Invalid VLAN [chars] in response.

Explanation The VLAN membership policy server (VMPS) has specified a VLAN name that is unknown to the switch. [chars] is the VLAN name.

Recommended Action Ensure that the VLAN exists on the switch. Verify the VMPS configuration by entering the **show vmps** privileged EXEC command.

Error Message PLATFORM_WCCP-4-SDM_MISMATCH: WCCP requires sdm template routing

Explanation The switch database management (SDM) routing template is not specified on the switch.

Recommended Action Specify the SDM routing template to be used. Enter the **sdm prefer routing** global configuration command, and then enter the **reload** privileged EXEC command to reload the switch.

Error Message WCCP-5-CACHEFOUND: Web Cache [IP_address] acquired.

Explanation The switch has acquired the specified web cache. [IP_address] is the web cache IP address.

Recommended Action No action is required.

Error Message WCCP-1-CACHELOST: Web Cache [IP_address] lost.

Explanation The switch has lost contact with the specified web cache. [IP_address] is the web cache IP address.

Recommended Action Verify the operation of the web cache by entering the **show ip wccp web-cache** privileged EXEC command.

Changed System Messages

The error explanation and action has changed for these system messages:

Error Message EC-5-CANNOT_BUNDLE1: Port-channel [chars] is down, port [chars] will remain stand-alone.

Explanation The aggregation port is down. The port remains standalone until the aggregation port is up. The first [chars] is the EtherChannel. The second [chars] is the port number.

Recommended Action Ensure that the other ports in the bundle have the same configuration.

Error Message ILPOWER-3-CONTROLLER_PORT_ERR:Controller port error, Interface Fa0/7:Power given, but link is not up.



Note

This message applies only to the Catalyst 3750 and 3560 switches.

Explanation The inline-power-controller reported an error on an interface.

Recommended Action Enter the **shutdown** and **no shutdown** interface configuration commands on the affected interfaces. Upgrade to Cisco IOS Release 12.1(14)EA1 or later, which provides an electrostatic discharge (ESD) recovery mechanism.

Deleted System Messages

These messages were deleted from all of the system message guides:

Error Message ACLMGR-2-NOVMR: Cannot create VMR data structures for access list [chars].

Error Message %VQPCLIENT-2-INITFAIL: Platform-specific VQP initialization failed. Quitting

Error Message %VQPCLIENT-2-IPSOCK: Could not obtain IP socket

Error Message %VQPCLIENT-7-NEXTSERV: Trying next VMPS [IP_address]

Error Message %VQPCLIENT-7-PROBE: Probing primary server [IP_address]

Error Message %VQPCLIENT-2-PROCFAIL: Could not create process for VQP. Quitting

Error Message %VQPCLIENT-7-RECONF: Reconfirming VMPS responses

Error Message %VQPCLIENT-2-SHUTDOWN: Interface [chars] shutdown by VMPS

Error Message %VQPCLIENT-3-THROTTLE: Throttling VLAN change on [chars]

Updates to the Catalyst 3750, 3560, and 2960 Hardware Installation Guide

Cisco Ethernet Switches are equipped with cooling mechanisms, such as fans and blowers. However, these fans and blowers can draw dust and other particles, causing contaminant buildup inside the chassis, which can result in a system malfunction.

You must install this equipment in an environment as free as possible from dust and foreign conductive material (such as metal flakes from construction activities).

These standards provide guidelines for acceptable working environments and acceptable levels of suspended particulate matter:

- Network Equipment Building Systems (NEBS) GR-63-CORE
- National Electrical Manufacturers Association (NEMA) Type 1
- International Electrotechnical Commission (IEC) IP-20

This applies to all Cisco Ethernet switches except for these compact models:

- Catalyst 3560-8PC switch—8 10/100 PoE ports and 1 dual-purpose port (one 10/100/1000BASE-T copper port and one SFP module slot)
 - Catalyst 2960-8TC switch—8 10/100BASE-T Ethernet ports and 1 dual-purpose port (one 10/100/1000BASE-T copper port and one SFP module slot)
 - Catalyst 2960G-8TC switch—7 10/100/100BASE-T Ethernet ports and 1 dual-purpose port (one 10/100/1000BASE-T copper port and one SFP module slot)

Update to the Regulatory Compliance and Safety Information for the Catalyst 2960 Switch

This warning applies to the Catalyst 2960 24- and 48-port switches:

Statement 266—Switch Installation Warning



Warning

To comply with safety regulations, mount switches on a wall with the front panel facing up.
Statement 266

Waarschuwing

Om te voldoen aan de veiligheidsvoorschriften dient u de schakelaars op een muur te monteren met het voorpaneel omhoog.

Varoitus

Turvallisuusmääräykset edellyttävät, että kytkimet kiinnitetään seinään etupaneeli ylöspäin.

Attention

Pour satisfaire aux dispositions de sécurité, installez les commutateurs muraux avec le panneau frontal vers le haut.

Warnung

Zur Einhaltung der Sicherheitsvorschriften die Schalter so an einer Wand montieren, dass die Frontplatte nach oben zeigt.

Avvertenza

In conformità ai regolamenti di sicurezza, installare i dispositivi switch a muro con il pannello frontale rivolto in su.

Advarsel

For å etterkomme sikkerhetsreglene skal brytere monteres på en vegg med frontpanelet vendt opp.

Aviso

Para cumprir com os regulamentos de segurança, faça a montagem de switches em uma parede com o painel frontal virado para cima.

¡Advertencia!

Para cumplir con las reglas de seguridad, instale los interruptores en una pared con el panel del frente hacia arriba.

Varning!

För att uppfylla säkerhetsföreskrifter skall switcharna monteras på en vägg med frampanelen riktad uppåt.

A biztonsági előírások betartása érdekében a kapcsolókat úgy szerelje a falra, hogy az előlapjuk felfelé nézzen.

Предупреждение В соответствии с положениями безопасности установите переключатели на стене передней панелью наружу.

警告 为符合安全规章，请将切换开关安装在墙上，前面板朝上。

警告 安全既定に準拠するために、フロントパネルを上向きにしてスイッチを壁にマウントします。

Updates to the Catalyst 3750 Getting Started Guide

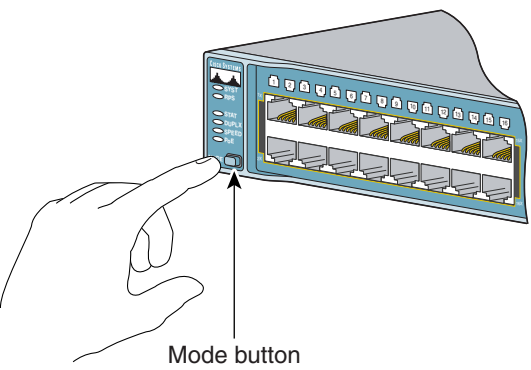
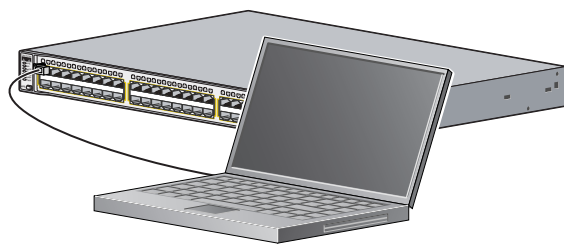
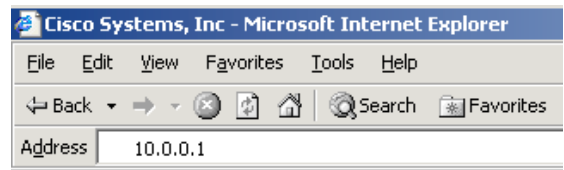
The Express Setup configuration windows were updated in the getting started guide. This is the complete procedure:

Running Express Setup

When you first set up the switch, you should use Express Setup to enter the initial IP information. This enables the switch to connect to local routers and the Internet. You can then access the switch through the IP address for further configuration.

To run Express Setup:

- | | |
|---------------|---|
| Step 1 | <p>Make sure that nothing is connected to the switch.</p> <p>During Express Setup, the switch acts as a DHCP server. If your PC has a static IP address, change your PC settings before you begin to temporarily use DHCP.</p> |
| Step 2 | <p>Power the switch by connecting the supplied AC power cord to the switch power connector and to a grounded AC outlet.</p> |
| Step 3 | <p>When the switch powers on, it begins the power-on self-test (POST). During POST, the LEDs blink while tests verify that the switch functions properly.</p> <p>Wait for the switch to complete POST, which can take several minutes.</p> |
| Step 4 | <p>Verify that POST has completed by confirming that the SYST LED remains green. If the switch fails POST, the SYST LED turns amber.</p> <p>POST errors are usually fatal. Contact your Cisco technical support representative if your switch fails POST.</p> |

<p>Step 5 Press and hold the Mode button for 3 seconds. When all of the LEDs left of the Mode button turn green, release the Mode button.</p> <p>If the LEDs left of the Mode button begin to blink after you press the button, release it. Blinking LEDs mean that the switch has already been configured and cannot go into Express Setup mode. For more information, see the “Resetting the Switch” section.</p>	 <p>Mode button</p>
<p>Step 6 Verify that the switch is in Express Setup mode by confirming that all LEDs left of the Mode button are green. (On some models, the RPS and PoE LEDs remain off.)</p>	
<p>Step 7 Connect a Category 5 Ethernet cable to any 10/100 or 10/100/1000 Ethernet port on the switch front panel.</p> <p>Connect the other end of the cable to the Ethernet port on your PC.</p>	 <p>DHCP-enabled PC</p>
<p>Step 8 Verify that the switch and PC Ethernet ports LEDs are green.</p> <p>Wait 30 seconds.</p>	
<p>Step 9 Start a web browser on your PC. Enter the IP address 10.0.0.1 in the web browser, and press Enter.</p>	

The Express Setup page appears. If it does not appear, see the “In Case of Difficulty” section for help.

The screenshot shows the 'Express Setup' page with two tabs: 'Basic Settings' and 'Advanced Settings'. The 'Basic Settings' tab is active, displaying two sections: 'Network Settings' and 'Optional Settings'.

Network Settings:

- Management Interface (VLAN ID): 1
- IP Address: [Four input boxes for IP address]
- Subnet Mask: 255.255.255.0 (with a dropdown arrow)
- Default Gateway: [Four input boxes for gateway address]
- Switch Password: [Input box]
- Confirm Switch Password: [Input box]

Optional Settings:

- Host Name: Switch
- System Date (DD/MMM/YYYY): [Three dropdown menus for date]
- System Time (HH:MM): [Two dropdown menus for time]
- Time Zone: [Dropdown menu]
- Daylight Saving Time: ☐ Enable

Step 10 Enter this information in the **Network Settings** fields:

In the **Management Interface (VLAN ID)** field, the default is 1. Enter a new VLAN ID only if you want to change the management interface through which you manage the switch. The VLAN ID range is 1 to 1001.

In the **IP Address** field, enter the IP address of the switch. In the **IP Subnet Mask** field, click the drop-down arrow, and select an **IP Subnet Mask**.

In the **Default Gateway** field, enter the IP address for the default gateway (router).

Enter your password in the **Switch Password** field. The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows embedded spaces, but does not allow spaces at the beginning or end. In the **Confirm Switch Password** field, enter your password again.

Step 11 (Optional) You can enter the **Optional Settings** information now or enter it later by using the device manager interface:

- In the **Host Name** field, enter a name for the switch. The host name is limited to 31 characters. Embedded spaces are not allowed.
- Enter the date, time, and time zone information in the **System Date**, **System Time**, and **Time Zone** fields. Click **Enable** to enable daylight saving time.

- Step 12** (Optional) Click the **Advanced Settings** tab on the Express Setup window, and enter the advanced settings now or enter them later by using the device manager interface.

- Step 13** (Optional) Enter this information in the **Advanced Setting** fields:

- In the **Telnet Access** field, click **Enable** if you are going to use Telnet to manage the switch by using the command-line interface (CLI). If you enable Telnet access, you must enter a Telnet password.
- In the **Telnet Password** field, enter a password. The Telnet password can be from 1 to 25 alphanumeric characters, is case sensitive, allows embedded spaces, but does not allow spaces at the beginning or end. In the **Confirm Telnet Password** field, re-enter the Telnet password.
- In the **SNMP** field, click **Enable** to enable Simple Network Management Protocol (SNMP). Enable SNMP only if you plan to manage switches by using CiscoWorks 2000 or another SNMP-based network-management system.
- If you enable SNMP, you must enter a community string in the **SNMP Read Community** field, the **SNMP Write Community** field, or both. SNMP community strings authenticate access to MIB objects. Embedded spaces are not allowed in SNMP community strings. When you set the SNMP read community, you can access SNMP information, but you cannot modify it. When you set the SNMP write community, you can both access and modify SNMP information.
- In the **System Contact** and **System Location** fields, enter a contact name and the wiring closet, floor, or building where the switch is located.

- Step 14** (Optional) You can enable Internet Protocol version 6 (IPv6) on the switch. From the Advanced Settings tab, check the **Enable IPv6** check box.



Note Enabling IPv6 restarts the switch when you complete Express Setup.

Step 15 To complete Express Setup, click **Submit** from the Basic Settings or the Advanced Settings tab to save your settings, or click **Cancel** to clear your settings.

When you click **Submit**, the switch is configured and exits Express Setup mode. The PC displays a warning message and tries to connect with the new switch IP address. If you configured the switch with an IP address that is in a different subnet from the PC, connectivity between the PC and the switch is lost.

Step 16 Disconnect the switch from the PC, and install the switch in your production network. See the “Managing the Switch” section for information about configuring and managing the switch.

If you need to rerun Express Setup, see the “Resetting the Switch” section.

Updates to the Regulatory Compliance and Safety Information for the Catalyst 3750 Switch

These statements were added to both the *Regulatory Compliance and Safety Information for the Catalyst 3750 Switch* and the *Catalyst 3750 Switch Hardware Installation Guide*:

Statement 371—Power Cable and AC Adapter

Statement 377—Temperature of the Removed SFP Module Might be Hot



Warning

When the Catalyst 3750-12S switch and 100BASE-FX MMF small form-factor pluggable (SFP) module (model number GLC-GE-100FX) are running, the surface temperature of the removed SFP module might be hot. Statement 377

Waarschuwing

Wanneer de Catalyst 3750-12S-switch en 100BASE-FX MMF small form-factor pluggable (SFP)-module (modelnummer GLC-GE-100FX) aanstaan, kan de oppervlaktetemperatuur van de verwijderde SFP-module heet zijn.

Varoitus

Kun Catalyst 3750-12S -kytkin ja irrotettava SFP-moduuli (small form-factor pluggable) 100BASE-FX MMF (mallinumero GLC-GE-100FX) ovat käynnissä, irrotetun SFP-moduulin pinta saattaa olla kuuma.

Attention

Lorsque le commutateur Catalyst 3750-12S et le petit module du lien montant SFP (Small Form-Factor Pluggable) 100BASE-FX MMF (modèle GLC-GE-100FX) fonctionnent, la surface du module SFP retiré peut être chaude.

Warnung	Wenn der Catalyst 3750-12S Switch und das 100BASE-FX MMF-SFP (small form-factor pluggable)-Modul (Typennummer GLC-GE-100FX) ausgeführt werden, ist die Oberflächentemperatur des entfernten SFP-Moduls möglicherweise sehr hoch.
Avvertenza	Quando sono in esecuzione lo switch Catalyst 3750-12S e il modulo SFP (Small Form-factor Pluggable) 100BASE-FX MMF (numero modello GLC-GE-100FX), la temperatura della superficie del modulo SFP rimosso può risultare elevata.
Advarsel	Når Catalyst 3750-12S-bryteren og SFP-modulen (small form-factor pluggable) 100BASE-FX MMF (modell nummer GLC-GE-100FX) kjører, kan overflatetemperaturen på den eksterne SFP-modulen bli varm.
Aviso	Quando o switch Catalyst 3750-12S e o módulo 100BASE-FX MMF small form-factor pluggable (SFP) (modelo GLC-GE-100FX) estão em funcionamento, a temperatura da superfície do módulo SFP pode ser elevada.
¡Advertencia!	Quando el switch Catalyst 3750-12S y el módulo de acoplamiento de factor de forma pequeño 100BASE-FX MMF (SFP), (número de modelo GLC-GE-100FX) se ejecutan, la temperatura de la superficie del módulo SFP extraído puede ser caliente.
Varning!	Når Catalyst 3750-12S-växeln och SFP-modulen 100BASE-FX MMF (modellnummer GLC-GE-100FX) körs, kan ytan på den borttagna SFP-modulen bli varm.
A Catalyst 3750-12S switch és a 100BASE-FX MMF SFP (small form-factor pluggable) modul (cikkszám: GLC-GE-100FX) működése közben az eltávolított SFP modul felülete forró lehet.	
Предупреждение	При работе коммутатора Catalyst 3750-12S совместно с SFP-модулем с многомодовым оптоволоконным кабелем 100BASE-FX MMF (модель GLC-GE-100FX) может повышаться температура поверхности удаленного SFP-модуля .
警告	Catalyst 3750-12S 交换机和 100BASE-FX MMF 小型可插拔 (SFP) 模块 (模块编号 GLC-GE-100FX) 正在运行时, 取出的 SFP 模块可能表面温度很高。
警告	Catalyst 3750-12Sスイッチおよび100BASE-FX MMF Small Form-Factor Pluggable (SFP)モジュール (モデル番号GLC-GE-100FX)が実行されている場合、取り外されたSFPモジュールの表面温度が高温になることがあります。

This warning replaces Statement 100C:

Statement 370—Attaching the Cisco RPS to the RPS Receptacle



Warning

Attach only the following Cisco RPS model to the RPS receptacle:

PWR-RPS2300, PWR675-AC-RPS-N1= Statement 370

Waarschuwing

Sluit alleen het volgende Cisco RPS-model aan op de RPS-ontvanger:

PWR-RPS2300, PWR675-AC-RPS-N1=

Varoitus

Kiinnitä vain seuraava Cisco RPS malli RPS-astiaan:

PWR-RPS2300, PWR675-AC-RPS-N1=

Attention

Raccordez le modèle Cisco RPS suivant uniquement au connecteur RPS :

PWR-RPS2300, PWR675-AC-RPS-N1=

Warnung

Schließen Sie ausschließlich das folgende Cisco RPS-Modell an die Anschlussstelle für die redundante Stromversorgung an.

PWR-RPS2300, PWR675-AC-RPS-N1=

Avvertenza

Collegare soltanto il seguente modello Cisco RPS alla presa RPS:

PWR-RPS2300, PWR675-AC-RPS-N1=

Advarsel

Du må bare koble følgende Cisco RPS-modell til RPS-mottakeren:

PWR-RPS2300, PWR675-AC-RPS-N1=

Aviso

Introduza apenas o seguinte modelo RPS da Cisco no receptáculo RPS:

PWR-RPS2300, PWR675-AC-RPS-N1=

¡Advertencia!

Acople únicamente el siguiente modelo Cisco RPS al receptáculo RPS:

PWR-RPS2300, PWR675-AC-RPS-N1=

Varning!

Bifoga endast följande Cisco RPS-modell till RPS-behållaren:

PWR-RPS2300, PWR675-AC-RPS-N1=

Csak az alábbi Cisco RPS modellt csatlakoztassa az RPS-csatlakozóhoz:

PWR-RPS2300, PWR675-AC-RPS-N1=

Предупреждение

К розетке RPS можно подключать только следующую модель Cisco RPS:

PWR-RPS2300, PWR675-AC-RPS-N1=

警告

仅附加下列 Cisco RPS 模型到 RPS 插座:

PWR-RPS2300, PWR675-AC-RPS-N1=

警告

RPS レセプタクルに接続できるのは、次の Cisco RPS モデルのみです:

PWR-RPS2300, PWR675-AC-RPS-N1=

Related Documentation

These documents provide complete information about the Catalyst 3750, 3560, and 2960 switches and the Cisco EtherSwitch service modules and are available at Cisco.com:

- http://www.cisco.com/en/US/products/hw/switches/ps5023/tsd_products_support_series_home.html
- http://www.cisco.com/en/US/products/hw/switches/ps5528/tsd_products_support_series_home.html
- http://www.cisco.com/en/US/products/ps6406/tsd_products_support_series_home.html

These documents provide complete information about the Catalyst 3750 switches and the Cisco EtherSwitch service modules:

- *Catalyst 3750 Switch Software Configuration Guide*
- *Catalyst 3750 Switch Command Reference*
- *Catalyst 3750, 3560, 3550, and 2960 Switch System Message Guide*
- *Catalyst 3750 Switch Hardware Installation Guide*
- *Catalyst 3750 Getting Started Guide*
- *Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Catalyst 3750 Switch*

These documents provide complete information about the Catalyst 3750G Integrated Wireless LAN Controller Switch and the integrated wireless LAN controller and are available at cisco.com:

- *Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide*
- *Release Notes for Cisco Wireless LAN Controller and Lightweight Access Point, Release 4.0.x.0*
- *Cisco Wireless LAN Controller Configuration Guide, Release 4.0*
- *Cisco Wireless LAN Controller Command Reference, Release 4.0*

These documents provide complete information about the Catalyst 3560 switches:

- *Catalyst 3560 Switch Software Configuration Guide*
- *Catalyst 3560 Switch Command Reference*
- *Catalyst 3750, 3560, 3550, and 2960 Switch System Message Guide*
- *Catalyst 3560 Switch Hardware Installation Guide*
- *Catalyst 3560 Switch Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Catalyst 3560 Switch*

These documents provide complete information about the Catalyst 2960 switches and are available on Cisco.com:

- *Catalyst 2960 Switch Software Configuration Guide*
- *Catalyst 2960 Switch Command Reference*
- *Catalyst 3750, 3560, 3550, and 2960 Switch System Message Guide*
- *Catalyst 2960 Switch Hardware Installation Guide*
- *Catalyst 2960 Switch Getting Started Guide*
- *Catalyst 2960 Switch Getting Started Guide*—available in English, simplified Chinese, French, German, Italian, Japanese, and Spanish

- *Regulatory Compliance and Safety Information for the Catalyst 2960 Switch*
- *Regulatory Compliance and Safety Information for the Catalyst 2960 Switch*

For other information about related products, see these documents:

- Device manager online help (available on the switch)
- *Getting Started with Cisco Network Assistant*
- *Release Notes for Cisco Network Assistant*
- *Cisco RPS 300 Redundant Power System Hardware Installation Guide*
- *Cisco RPS 675 Redundant Power System Hardware Installation Guide*
- For more information about the Network Admission Control (NAC) features, see the *Network Admission Control Software Configuration Guide*
- *Cisco Small Form-Factor Pluggable Modules Installation Notes*
- *Cisco CWDM GBIC and CWDM SFP Installation Note*
- These compatibility matrix documents are available from this Cisco.com site:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

- *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*
- *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix*
- *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*
- *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the “[Obtaining Documentation and Submitting a Service Request](#)” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008–2009 Cisco Systems, Inc. All rights reserved.

